



Encryption 101

Eight common encryption issues facing organizations today

March 08

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

© Copyright 2008 Entrust. All rights reserved.

Table of Contents

1	Introduction	1
2	Why is encryption important today?	1
	Losses continue, costs escalate.....	1
	Data security regulations and privacy laws are stronger than ever.....	2
	Peer pressure and partnerships	2
3	Eight common encryption issues facing organizations	3
	IBE, PKI or a hybrid	3
	Securing the mobile workforce	5
	Sharing encrypted data outside your organization	5
	End-to-end versus gateway encryption	7
	Audits and logs	8
	Can laptop full-disk encryption alone provide enough protection?.....	8
	How do you make encryption part of everyday business operations?	9
	Can access control secure information?	10
4	Conclusion.....	11
5	About Entrust	11

1 Introduction

Pressures are mounting for organizations to implement encryption solutions. From regulatory compliance, to partner demands and the staggering costs of data loss, encryption projects are on the rise. This paper explores the most common issues organizations face when making decisions about which types of encryption solutions to use. Having a cross-organizational view of the myriad of encryption requirements can seem daunting, but will ensure the selected solution can provide what you need while minimizing IT overhead and reducing redundancy. Look for solutions that can cover a range of encryption options, but be wary of point solutions that may seem to be a simple choice but provide limited functionality.

2 Why is encryption important today?

Using encryption as a tool to protect information and prevent data loss is certainly not a new tactic. From protecting files, folders and e-mail to full-disk encryption, encryption technologies have been leveraged for years. There are several key factors happening now that make encryption more relevant than ever. From snooping employees to compliance pressure, today's need for encryption focuses around three primary issues.

Losses continue, costs escalate

Data breaches are happening around the world on an almost-daily basis. According to privacyrights.org, more than 218 million data records of U.S. residents have been exposed due to security breaches since January 2005. This does not include breaches where the number of records were "unknown" or breaches that went unreported.

Not all breaches are from external sources. Research tells us that one third of IT managers admit to snooping through corporate data and that the actual number is likely even higher. Other studies suggest that the overwhelming majority of data breaches originate from inside the organization.

New research indicates that as breaches occur more often, they also are getting increasingly costly:

According to the study, data breach incidents cost companies \$197 per compromised customer record in 2007, compared to \$182 in 2006. Lost business opportunity, including losses associated with customer churn and acquisition, represented the most significant component of the cost increase, rising from \$98 in 2006 to \$128 in 2007 — a 30 percent increase.

The Ponemon Institute

Encryption Terms Explained ...

Encryption – When you encrypt a file, folder or e-mail, you apply a mathematical function that transforms every character in the file into some other character, rendering it unreadable. This means no one, including you, can read the file until it is decrypted.

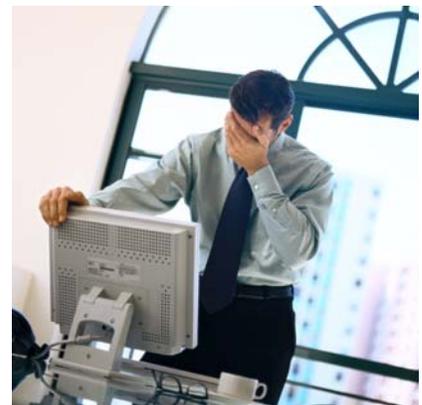
Keys - Encrypting something requires an encryption key, typically called a public key that essentially "locks" the file to anyone but those possessing a second type of key called a decryption key or private key that can "unlock" the file.

Key pair - Refers to both the public (encryption) key and private (decryption) key.

Certificates - Users are issued a certificate that acts as a secure electronic identity and contains their public key. Private keys should be securely stored separately.

Key and Certificate management - Consider the certificates and private keys that must be issued to every user who will be encrypting or decrypting. Managing these keys and certificates can be complex. Tasks such as adding new employees to the system or removing employees who have left, backing up and recovering data, and managing lost passwords will be part of the daily management of this system. Manually managing the keys and certificates used by an encryption system is virtually impossible. Key and certificate management often refers to a set of capabilities found in encryption products to reduce this administrative burden.

PKI – One of the leading approaches to key and certificate management is a public key infrastructure (PKI). It provides many security services including encryption, digital signatures and authentication, and has robust management and administration capabilities.



While \$197 per record might seem like an insignificant amount, when it is multiplied by an entire employee or customer population, costs mount at an alarming rate.

Data security regulations and privacy laws are stronger than ever

Almost all organizations must meet specific security and data protection requirements from some regulatory body, including:

Disclosure Laws — California Senate Bill SB 1386, and many others like it, require mandatory notification of affected parties in the event of unauthorized acquisition of residents' personal information that is stored in electronic form. The California legislation is explicit in noting that notification is not required if the information is encrypted, known as the "safe harbor" clause. In addition, more than 20 states have enacted their own version of the California legislation including New York and Texas. Several bills are also under review at the federal level in the U.S., and the European Commission has proposed a directive to require providers of "electronic communications networks or services" to notify customers of personal data breaches.



Payment Card Industry Data Security Standard — PCI DSS was updated in 2006 to include stricter application standards beginning in January 2008. Merchants face steep fines if they are found not to be compliant, and Visa recently admitted that only 60 percent of their Level 1 merchants are compliant. The cornerstone of the PCI guidelines is the requirement to encrypt customer data while it is both stored and in transit.

The Health Insurance Portability and Accountability Act — HIPAA seeks to ensure privacy rights and the security of health information. The HIPAA security standard covers what safeguards must be in place to protect electronic patient information. Organizations must ensure that private health information is protected both at rest and in transit.

Gramm Leach Bliley Act — The GLBA, or Financial Services Modernization Act of 1999, includes provisions to protect consumers' personal financial information held by financial institutions. GLBA instructs organizations to take precautions to secure data whether it is consumer information or financial reporting systems, no matter where it resides or is used.

Peer pressure and partnerships

More and more organizations are mandating encryption not only for themselves but for partner organizations they do business with. For example, some banks will not transact with other organizations unless they have the capability to send and receive encrypted e-mails.

Contractual obligations require it.

Many businesses are including requirements for their partners to encrypt sensitive data in transit or at rest, especially if that data contains personal information about their customers or their employees.¹

Forrester Research

The ability to not only secure data internal to the organization but also while in transit beyond the border of the organization is increasingly becoming a priority.

¹ "Adopting An Enterprise Approach To Encryption," March 2007, Paul Stamp, Forrester Research

3 Eight common encryption issues facing organizations

While data loss, regulatory compliance and peer pressure are pushing organizations to take action on encryption at a corporate level, many organizations are discovering that it is already being used in small user groups throughout the organization. It can seem that it might be easier to just add encryption to one workgroup, one data type at a time. But adding additional small point solutions that only offer full-disk encryption, for example, is unlikely to provide protection for the range of data types used by your organization.

There are several types of data encryption:

- **File and folder encryption** – sometimes called desktop encryption, allows users to encrypt files or folders residing on their PCs, laptops or portable storage devices and other media
- **E-mail encryption** – protects e-mail messages as they travel both within a corporate network, and perhaps more importantly beyond the boundaries of the corporate network
- **Full-disk encryption** – encrypts an entire hard drive rather than individual files or messages and is popular for laptops used by mobile workers
- **Mobile data encryption** – encrypts data stored on devices such as PDAs and smart phones; e-mail encryption is also used by mobile devices such as the RIM BlackBerry
- **Application encryption** – encrypts data stored within a custom application such as a payroll system

While there may be specific point solutions that provide encryption for just one of these data types, increasingly organizations are looking at the total package of data that must be protected while at rest or while in transit. They require solutions that can provide a range of encryption options to meet regulatory and partner pressures today and in the future.

Once you begin to look beyond a small point solution for encryption, most people face standard issues. From understanding the differences between encryption methods, to determining whether or not you need end-to-end e-mail encryption; this paper's aim is to assist in understanding encryption so that you can make the right decisions for your organization's encryption strategy and program.

IBE, PKI or a hybrid: Understanding encryption methodologies and standards so you can choose

There are a broad range of encryption solutions available today and they are often difficult to categorize and compare. Each solution uses one of four standard encryption methodologies. Each methodology offers a different approach to the types of data that can be protected, how to manage the user experience and the place that an encryption solution will occupy in your overall infrastructure.

Some methodologies have been developed to be simple point solutions that manage one small aspect of encryption. Others are more robust and offer a more comprehensive set of encryption tools. Use the following to help understand what kind of solutions you want to evaluate and which ones you might want to avoid.



Methodology & Uses	Overview	Strengths	Weaknesses
<p>Public key infrastructure (PKI) is used for a range of encryption types including:</p> <ul style="list-style-type: none"> • File & folder • E-mail • Full-disk • Mobile e-mail • Mobile data 	<ul style="list-style-type: none"> • PKI issues and manages keys and certificates • Provides end-to-end security for data 	<ul style="list-style-type: none"> • Robust, comprehensive management • Provides security services beyond encryption including digital signatures and authentication • Standards-based and scaleable 	<ul style="list-style-type: none"> • Perceived as complex • Costly
<p>Identity Based Encryption (IBE) is typically used for:</p> <ul style="list-style-type: none"> • E-mail • Mobile e-mail 	<ul style="list-style-type: none"> • IBE is a public-key cryptosystem that can use any string as a valid public key • For example, e-mail addresses and dates can be public keys. 	<ul style="list-style-type: none"> • Simple point solution • Easy to understand • There are no public keys because text strings such as the e-mail address are considered the public key 	<ul style="list-style-type: none"> • Not based on industry standards • Provides encryption only and no other services such as digital signatures • Closed system using proprietary technology • Client software required for all users including external recipients of data • Decryption keys stored insecurely • Can't work with other methodologies such as "Encrypting the Pipe"
<p>"Encrypting the Pipe" using Transport Layer Security (TLS) is typically used for:</p> <ul style="list-style-type: none"> • E-mail • Mobile e-mail 	<ul style="list-style-type: none"> • Encrypts the pipe that transports messages from the sender's e-mail gateway to recipient's e-mail gateway • Does not encrypt messages, but provides protection during transit 	<ul style="list-style-type: none"> • Simple point solution • Native to Exchange • Easy to use and invisible to the user • Focuses on the most vulnerable part of message delivery 	<ul style="list-style-type: none"> • Individual messages are not encrypted • Cannot secure data or messages within an organization • Assumes outside organizations also use gateway encryption • Cannot work with other methodologies such as IBE
<p>Hybrid or PKI PLUS is used for a range of encryption types including:</p> <ul style="list-style-type: none"> • File & folder • E-mail • Full-disk • Mobile e-mail • Mobile data 	<ul style="list-style-type: none"> • Uses a robust PKI platform combined with simplified management and streamlined operations • Provides end-to-end security for all types of data • Flexibility allows choice for e-mail including gateway- to-gateway encryption 	<ul style="list-style-type: none"> • Easy to set up and manage, masks complexity • Robust user and key management • Flexible for all types of e-mail delivery including Web-based 	<ul style="list-style-type: none"> • Flexibility can be seen as complex

Checklist

Before choosing one of these encryption methodologies, determine:

- How important is flexibility to your organization?
- Do data and messages need to be encrypted at rest as well as in transit?
- Do you want to distribute and manage client-side software to every user inside and outside your organization?
- Could your requirements expand to include digital signatures?
- Does your organization require the use of standards-based, non-proprietary software components?

Securing the mobile workforce

More and more organizations are arming employees with the tools to work from anywhere, any time. Employees are accessing the corporate network from hotels, coffee shops and their homes. There are fundamental changes in our collective work habits as activities such as evening e-mail checking and on-the-go report-writing are now a part of how we work on a daily basis.

IDC Predicts the Number of Worldwide Mobile Workers to Reach 1 Billion by 2011 ...



Pressure on companies to provide work/life balance programs for employees combined with advances in mobile technologies is increasing the number of mobile workers in the U.S. and around the world. By year-end 2011, IDC expects nearly 75 percent of the U.S. workforce will be mobile.²

Mobile computing devices such as PDAs, smart phones and BlackBerrys give employees the flexibility and freedom they need to be more productive. As more mobile workers work from anywhere, at any time, the corporate security architecture starts to lose the power to protect and prevent incidents. A mobile worker's lost PDA or the BlackBerry they left in a taxi are often beyond IT's ability to control and protect. Make sure your encryption strategy deals with your mobile workers, while not limiting how they work.

Look for encryption solutions that are able to extend to all of the devices your users access sensitive data from. E-mail encryption needs to work with BlackBerry and other smart phones. Encryption solutions should be persistent so that encrypted data stays encrypted while in transit or at rest on a mobile device, and decrypted only when needed by the user.

Checklist

- Do your users access sensitive information from mobile devices?
- How is information protected while in transit to mobile devices or while residing on mobile devices?
- If you encrypt e-mail, will BlackBerry users be able to use the S/MIME functionality to view it? Can mobile phone users read and respond to those messages?

Sharing encrypted data outside your organization: Understanding e-mail encryption choices

Encryption solutions use several message formats when they are sending encrypted messages. They use different approaches to allow recipients to receive, decrypt and respond to encrypted message, each with their own strengths and weaknesses. Understanding the inherent strengths and weaknesses of each message format may sound complex but is essential to ensuring you are selecting an encryption solution that works in the appropriate scenarios. Use the following to assess proposed solutions and help make the right decision for your organization.

² ["IDC Predicts the Number of Worldwide Mobile Workers to Reach 1 Billion by 2011,"](#) January 2008

Message Formats	Overview	Strengths	Weaknesses
S/MIME Secure / Multipurpose Internet Mail Extensions	<ul style="list-style-type: none"> • A format for messages that includes certificate and message content in specific manner • Developed by security vendors • As the industry standard, all leading e-mail clients understand S/MIME 	<ul style="list-style-type: none"> • Industry standard • Encrypted messages can appear directly in most e-mail client software application • Works with Microsoft® Outlook™ Web Access (OWA) 	<ul style="list-style-type: none"> • Most external recipients don't have an SMIME certificate and a certificate exchange is required in order to complete message sending/receiving • Can't reply within Outlook Web Access, leaving remote users with limited functionality
Client Software	<ul style="list-style-type: none"> • Instead of using native features of leading e-mail clients, some solutions require recipients to download software that decrypts the message or plugs into client software to facilitate the decryption 	<ul style="list-style-type: none"> • Some have integration with Outlook for native viewing of e-mails 	<ul style="list-style-type: none"> • Installing client software is cumbersome and difficult to support • It is inconvenient and users are unlikely to install software for one secure message • Does not work with OWA • Many organizations restrict what applications their users can download and install
OpenPGP	<ul style="list-style-type: none"> • A format for messages that includes certificate and message content in specific manner • Developed by an individual company rather than the industry 	<ul style="list-style-type: none"> • Encrypted messages can appear directly in most e-mail client software application 	<ul style="list-style-type: none"> • Most external recipients do not have an OpenPGP certificate and a certificate exchange is required in order to complete message sending/receiving • Can't reply within Outlook Web Access, leaving remote users with limited functionality
Web-based solutions	<ul style="list-style-type: none"> • Messages can be delivered to recipients either as a webmail inbox where the sending company stores and displays the message, or in an encrypted HTML attachment that the recipient opens in a secure browser session 	<ul style="list-style-type: none"> • The Web-based approach ensures ubiquitous access 	<ul style="list-style-type: none"> • If messages are pushed to an encrypted HTML attachment, users should have to be online to decrypt or risk a "brute-force attack" • Not all Web-based solutions allow recipients to save their message in their own e-mail application • Some Web-based messages may include javascript or code that is commonly blocked by anti-SPAM devices
Adobe Acrobat	<ul style="list-style-type: none"> • Adobe Acrobat documents use a proprietary file type that can be password-protected 	<ul style="list-style-type: none"> • Adobe Acrobat is almost ubiquitous • Simple, easy method to share documents like statements outside the boundary of the corporate network 	<ul style="list-style-type: none"> • Management issues such as password management and certificate revocation • Susceptible to brute-force attack • Early versions of Acrobat used weaker encryption; although it is now strong, there may be negative perceptions

Checklist

- How important is the use of industry standards to your organization?
- What IT resources will be dedicated to the management of your encryption system? Do you want an automated or manual system?
- Do your e-mail recipients need to be able to respond securely?
- Do your mobile workers rely on Web access to their e-mail? Will the encryption solution work for them?
- Do you want to distribute and manage client-side software to every user inside and outside your organization?

End-to-end versus gateway encryption: what you need to know

This is a very common dilemma for organizations looking to add encryption to e-mail. Organizations using encryption in the past had to rely on a client-side desktop application to perform encryption operations. Users had to manage certificates of people they wanted to send messages to. They were responsible for harvesting keys, managing encryption and any number of other technical tasks. Because messages were secured at the desktop and decrypted at the recipient's desktop, the process was considered end-to-end.

Gateway-based encryption has become the technology of choice for many organizations because certificate management and new delivery methods extended encryption to any e-mail user outside the organization. Gateway solutions provide protection at the most vulnerable point for the message as it was in transit, outside the boundaries of the corporate network.

For some organizations who deal with sensitive data, there will be islands of users who need end-to-end e-mail encryption. These users may need higher levels of assurance about message integrity or simply have increased security requirements. End-to-end encryption ensures security of messages for those users who are typically encrypting for within the organization and, therefore, can deal with some of the disadvantages of this type of solution — compatibility problems with gateway users, difficulties managing multiple desktops or problems with e-mail archiving systems.

It is important to consider these communities of users that insist on using end-to-end encryption, even if the rest of the organization's security needs can be met with gateway-based encryption. Although some encryption solutions can only provide one or the other, robust systems should be able to accommodate both.

Any gateway-based solution should be able to manage message delivery and encryption certificates on behalf of desktop users to give the whole organization the benefits of both platforms. Indeed, some gateway solutions take the hassle of managing the delivery out of the hands of the end-to-end user. A message is secured at the desktop and if the message is directed outside the organization the gateway solution can manage the certificate harvesting, delivery, etc.



There are now solutions that can manage messages secured with end-to-end encryption so they can be properly archived by leading e-mail archiving platforms. Also look for solutions that have

been integrated with content-control technologies to allow end-to-end encrypted messages to be scanned for compliance using a gateway appliance.

Checklist

- Review the level of security required for your e-mail encryption strategy.
- Are there certain users that may need end-to-end encryption such as your executive team?
- Perform an audit to determine if there are any “islands” that use desktop-based encryption today.

Audits and logs: how to keep auditors and compliance officers happy

Regulatory compliance must be proven. Organizational policy and security practices must be documented and detailed in audit trails and logs. In order to generate the reports required for these security audits, information must be systemically protected with robust encryption systems. Small point solutions such as Transport Layer Security (TLS) between gateways simply cannot provide the detailed reporting required by auditors and compliance officers.

Auditors need proof that a protected file was accessed, and who it was accessed by to comply with some regulations. Security auditors also want to ensure that encryption systems are secure. They look for enhanced security features such as multifactor authentication of users. They also expect industry best practices to be followed, including the use of technologies that meet standards such as FIPS 140. There are many solutions that claim to provide the level of reporting and audit-tracking needed, but as the requirements constantly evolve it is essential that your solution be flexible.

Checklist

- What types of information do you need to provide to compliance officers and auditors?
- Does the encryption system provide the types of reports and auditable logs you need?

Can laptop full-disk encryption alone provide enough protection?

Often organizations think that encrypting data on laptops with full-disk encryption will provide total protection of corporate data. Full-disk encryption, however, is focused on equipment that may be lost or stolen. It does not deal with data security while in use or when shared. Encrypting all the data on a laptop will certainly protect the information if the laptop is lost or stolen, providing it was fully shutdown and not in standby mode, but it does little to protect the data beyond that.



Once a laptop has been booted (decrypted), all files are available for use which may extend to copying, posting, e-mailing, etc. As soon as a user moves a file off that laptop to share or e-mail, that data is at risk. If a user decrypts a file and then emails it beyond the borders of the organization, the laptop encryption solution provides no protection. If the file is sent internally to a user who posts it on a shared network drive, there is no protection in place to prevent another employee from snooping or sending it to yet another unauthorized person.

Full-disk encryption for laptops can be an adequate tool for some organizations, but it does not provide protection of the data itself. It is important to think of data protection as a moving entity, that must be protected while in storage on a laptop but also while in transit. Employees rarely have sensitive data that only exists on their laptops and is never shared or emailed. Laptop encryption is focused on preventing data loss in a very limited set of loss or theft scenarios but we know that data can be compromised internally and more importantly while in transit.

Checklist

Before choosing laptop encryption alone, determine:

- Do data loss opportunities exist beyond theft/loss scenarios?
- Do users send and receive data files internally and externally?
- If yes, is the data protected in transit and beyond the borders of the organization?

How do you make encryption part of everyday business operations?

No matter which encryption solution you select, you cannot rely on individual users to ensure that it is used consistently. It is difficult to change user behavior and organizational policy is not enough to compel users to alter their typical behavior patterns and take action to encrypt.

Ensuring encryption is consistently used, in accordance with organizational policy and regulatory compliance, can be difficult if the encryption solution relies on the user to take action to encrypt, manage keys or certificates, or install software. Look for encryption solutions that remove the burden from the user and apply encryption consistently and in accordance with policy using things like:



- **Autonomous encryption** simply encrypts everything, automatically. Often used for internal e-mails, autonomous dedicates a lot of computing resources to encrypting and decrypting data that may or may not be sensitive. For some organizations subject to stringent regulations or dealing with highly sensitive material, this may be appropriate.
- **Transparent encryption** completes encryption operations without any direct action required by the user. Because a transparent operation does not affect the way users work, this is often an essential component for large deployments of encryption systems.
- **Content-control technologies** detect sensitive data and apply the appropriate encryption decision (to encrypt or not) to it.

Checklist

- Do you need to ensure consistent use of encryption across the organization?
- Can your encryption solution adapt to your changing policy and regulatory requirements without burdening users?

Can access control secure information?

Some organizations use access control instead of encryption to protect data from individuals not authorized to view or edit the data. Typically they use access control lists or rules-based access control schemes. It is important to understand what this type of protection provides and what it does not provide.

Controlling access can certainly stop a manager in marketing from looking at budget data from accounting. But can it stop someone in IT from looking at the same data? What if someone from accounting moves to marketing, will they still have access to the budget data? Who decides if this person's access should change?

The management and administration required to keep access control lists current is daunting. And this is only exacerbated by everyday factors like new data types that need to have access controls defined or peoples' changing roles within the organization. In addition, those administering the access rights will have a view of the information. Given that one third of all IT professionals have admitted to snooping, regulatory compliance can be compromised even though the data security has not been breached.

Standard security features like access control lists or operating system (OS) authentication offer inadequate protection when an attacker has physical access to a device storing sensitive unencrypted data, such as when a laptop or USB drive falls into the wrong hands. Increasingly, organizations need to encrypt stored data, especially if the device leaves the physical confines of the corporate environment.³

Forrester Research

Access controls are simply not designed to provide the level of protection delivered by most encryption technologies, nor can it provide any protection outside the boundaries of the corporate network. Access control may be useful for protecting access to applications or some data bases. For organizations with dynamic working groups and teams, changing data types and those moving sensitive data around the organization and beyond encryption provides more complete protection.

Checklist

- Does sensitive data always reside on centralized servers or is moved around the organization or sent outside of the organization?
- Do you have the IT power to administer and manage access control?
- Will your regulatory compliance be compromised if an IT employee snoops?

³ "Adopting an enterprise approach to encryption", March 6, 2007, Paul Stamp, Forrester Research

4 Conclusion

Increasing pressure to use encryption has many organizations initiating encryption projects. Data loss, regulatory requirements and partner demands all point to the need for an encryption platform that can respond to the pressure. Today's encryption technologies and solutions are sophisticated and are able to manage data protection duties across a wide range of data types, applications and user populations.

It is important to assess the global need for encryption across the entire organization when assessing solutions.

Keep a wider picture in mind when complying with specific mandates.

Many encryption deployments are reacting to the latest compliance mandate, and thus need to solve a specific problem. However, when complying with these mandates, it's important to remember that encryption requirements are likely to increase. So, you could be painting yourselves into a corner, or creating an administrative headache. Look for vendors that are not only able to solve the tactical problem at hand, but also help craft your future data security plans⁴.

Forrester Research

Point solutions might seem easier to implement in small workgroups for specific tasks but they cannot provide a workable, scalable solution to be used across the organization, nor can they provide the robust audit logs and reporting required by your compliance officer or security auditor. Look for solutions that can meet your requirements today and grow and change as future requirements are determined.

5 About Entrust

Entrust [NASDAQ: ENTU] secures digital identities and information for consumers, enterprises and governments in 1,700 organizations spanning 60 countries. Leveraging a layered security approach to address growing risks, Entrust solutions help secure the most common digital identity and information protection pain points in an organization. These include SSL, authentication, fraud detection, shared data protection and e-mail security. For information, call 888-690-2424, e-mail entrust@entrust.com or visit www.entrust.com.

⁴ "Adopting an enterprise approach to encryption", March 6, 2007, Paul Stamp, Forrester Research