

White Paper

The True Costs of E-mail Encryption

Trend Micro IBE (Identity-based) vs. PKI Encryption

By Jon Oltsik

June, 2010

This ESG White Paper was commissioned by Trend Micro and is distributed under license from ESG.

Contents

Executive Summary	3
E-mail Encryption: The Good, the Bad, and the Ugly	3
Identity-based E-mail Encryption: A Potential Breakthrough	4
Trend Micro Encryption.....	5
The Trend Micro IBE Cost Advantage	6
ESG’s E-mail Encryption Cost Model	7
Server Costs	7
E-mail Encryption Gateway Hardware Costs	7
Capital Cost for Software.....	7
Software Maintenance Cost	7
Software Client Installation Costs.....	7
Cost of E-mail Encryption Solution Installation	8
Cost of Developing User Training and Courseware	8
Cost of User Training	8
Help Desk Costs	8
IT Management and Operations Cost	9
Other Cost Considerations.....	10
The Bigger Truth	11

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change from time to time. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of the Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at (508) 482-0188.

Executive Summary

Do large organizations need an e-mail encryption solution? Yes, in almost all cases. Why? Every day, your organization exchanges sensitive, private, and regulated data with others via e-mail. Without encryption, this data is free and clear, all over the public Internet.

Given this, one would assume that many organizations are regularly deploying e-mail encryption solutions and negotiating encryption policies and processes with business partners. Unfortunately, this isn't the case: today's e-mail encryption solutions remain complex, so omnipresent e-mail encryption is next to impossible.

Currently, e-mail encryption is a bit of a paradox. Large organizations understand and want privacy, but e-mail encryption technology is too in-depth for mass usage. Fortunately things are changing. This paper concludes:

- **Existing e-mail encryption solutions are at the heart of the problem.** End-to-end email encryption solutions are supported by a full PKI infrastructure. This means implementing a full PKI back-end and distributing/managing digital certificates for each registered user. For IT organizations, PKI is costly and skills aren't readily available. This means training user on things like digital certificates, key security, public/private keys of e-mail recipients, and software functionality. Little wonder why so many organizations minimize their e-mail encryption investments or eschew them entirely.
- **Identity-based encryption (IBE) is an attractive alternative.** Key management doesn't have to be this complex anymore. New solutions based upon IBE eradicate the need for digital certificates by calculating key values based upon identity characteristics like a recipient's e-mail address. This can deliver the benefits of PKI without security researchers and PhDs to manage it.
- **[Trend Micro Encryption](#) stands out.** Yes, IBE solutions greatly simplify key management, but some products still require users to manage key servers and negotiate key exchange with external parties. Trend Micro Encryption is an exception to this rule; it backs its premise-based e-mail encryption clients and gateways with cloud services for key management, and external user registration. This makes Trend Micro Encryption one of the most effective and efficient e-mail encryption solutions available today.
- **Trend Micro's IBE solution benefits can add up to real cost savings.** For the purposes of this paper, ESG created a model to compare the costs of PKI and IBE solutions. Based upon assumptions and estimates, ESG's model calculates that Trend Micro Encryption can deliver a 78% savings over a PKI alternative.

E-mail Encryption: The Good, the Bad, and the Ugly

In spite of increasing investment in information security technology, publicly-disclosed data breaches continue unabated. There have been a total of 2,650 data breach incidents reported over the last five years (source: [datalossdb.org](#)). In 2009 alone, data breach incidents occurred at large public and private organizations like Heartland Payment Systems, the Federal Reserve Bank of New York, the Internal Revenue Service, and Aetna. According to the Privacy Rights Clearinghouse, the total number of records containing sensitive personal information exposed in data breach incidents exceeds 350 million (source: [privacyrights.org](#)).

All of these data breaches, along with general concern about data security, have driven numerous international, federal, state, and industry regulations aimed at protecting private records. In the United States, data privacy is now guided by federal regulations such as HIPAA and GLBA, international industry mandates like PCI DSS, and state regulations like Nevada NRS 590.970 and Massachusetts 210 CMR 17. Over the past few years, many countries' security/privacy regulations have become increasingly stringent, mandating that personal records must be encrypted at all times (i.e., data at rest and data in motion).

Of course, data security/privacy and associated regulations are nothing new. It would be safe to assume that most large organizations have already deployed safeguards like e-mail encryption for regulatory compliance and general best practices for data security. Unfortunately, this assumption is untrue. Many continue to circumvent e-mail encryption technology entirely or deploy and use the technology on a limited basis.

Why blatantly avoid an obvious solution like e-mail encryption? Because e-mail encryption technology carries some negative baggage as it can:

- **Interrupt business processes.** Since sensitive data often moves between organizations via e-mail, encryption means developing cross-organizational solutions. This can involve integrating multiple heterogeneous systems, creating a federated key management network, and training disparate users with varying skill sets. Planning alone can take months. Many avoid these intra-organizational efforts by implementing encryption in small pockets on an as-needed basis (“islands of email encryption”). Yes, this leads to interoperability headaches, but when it comes to e-mail encryption, CIOs often see this as the lesser of two evils.
- **Carry a high cost.** E-mail encryption solutions bring fairly extensive costs to purchase and implement. As previously stated, many products require a complete Public Key Infrastructure (PKI) that can involve multiple internal and web-facing servers, additional storage for encrypted e-mails, and numerous software licenses. Deploying these solutions can also be time consuming and complex, requiring the acquisition of new skills. In researching this topic, ESG found numerous organizations claiming that the hardware, software, and implementation cost of their e-mail encryption solutions exceeded budget estimates by up to 30% while deployment projects languished weeks or months behind schedule.
Require costly and specialized operations and support. Once installed, PKI-based e-mail encryption solutions require constant care and feeding for activities like help desk support, registering users, rotating user certificates, and maintaining certificate revocation lists. Large organizations estimate that this effort can consume about 40% of a full-time IT employee’s time.

Ultimately, all of these challenges lead to numerous and ongoing problems. Employees either don’t know which e-mails to encrypt or don’t know how to use their encryption software. To receive encrypted e-mails, external users are forced to create accounts and then view e-mails in an unfamiliar format. Meanwhile, IT administrators make mistakes like exposing the system’s master key or misconfiguring a firewall, denying access to external users. Given this mess, it is not hard to understand why many organizations are reluctant to embrace e-mail encryption beyond a minimal commitment.

Identity-based E-mail Encryption: A Potential Breakthrough

E-mail encryption problems have not gone unnoticed by the security industry. Many vendors claim they can avoid the problems described above by eliminating client-side requirements and addressing e-mail encryption with a gateway appliance. These appliances encrypt e-mails based upon pre-defined rules—when an e-mail contains electronic Patient Health Information (ePHI), social security numbers, or credit card numbers, gateway appliances filter packets, discover private data, and encrypt the e-mails accordingly.

Gateway appliances address some of the complexities described above, but do they provide comprehensive protection? Not really. As corporate governance becomes increasingly rigorous, many organizations now require e-mail encryption for internal communications between trusted users and groups. Since gateways generally sit at the network perimeter, appliances will be blind to this traffic without major, and usually illogical, changes to the network configuration. Furthermore, future regulations may mandate that e-mails containing sensitive data must be encrypted on an end-to-end basis from sender to receiver. Once again, gateway solutions alone aren’t enough.

So what’s needed? A solution offering the end-to-end security, privacy, and non-repudiation of PKI without the associated complexity. Fortunately, this type of solution exists today, based upon an encryption technology known as Identity-based Encryption (IBE). IBE is, in fact, a derivative of PKI, but it uses a simple identity attribute, like a recipient’s e-mail address, to generate a key public/private key pair. This eliminates a number of intricate tasks like generating, managing, rotating, and revoking digital certificates and thus addressing much of the system complexity described above. Additionally, users no longer need their own key pair before they can receive an e-mail. When an e-mail is sent to an unrecognized recipient, IBE creates a key pair on the fly based on the recipient’s e-mail address. To decrypt the e-mail, the recipient simply creates an account on a central system, receives a private key, and then reads the e-mail as always.

In general terms, IBE e-mail encryption solutions eliminate a good deal of the burden of certificate and key management, greatly simplifying implementation and operations. With many IBE solutions, however, some overhead remains; certain IBE products still require on-site key management systems that still require physical servers, storage capacity for encrypted e-mails, security safeguards, and ongoing maintenance. To operate across multiple organizations, these IBE systems may also require federation of homogeneous key servers. If one organization chooses another e-mail encryption system, the encryption network breaks down. Are these IBE solutions better than standard PKI? Yes, but architectural shortcomings make them far from perfect.

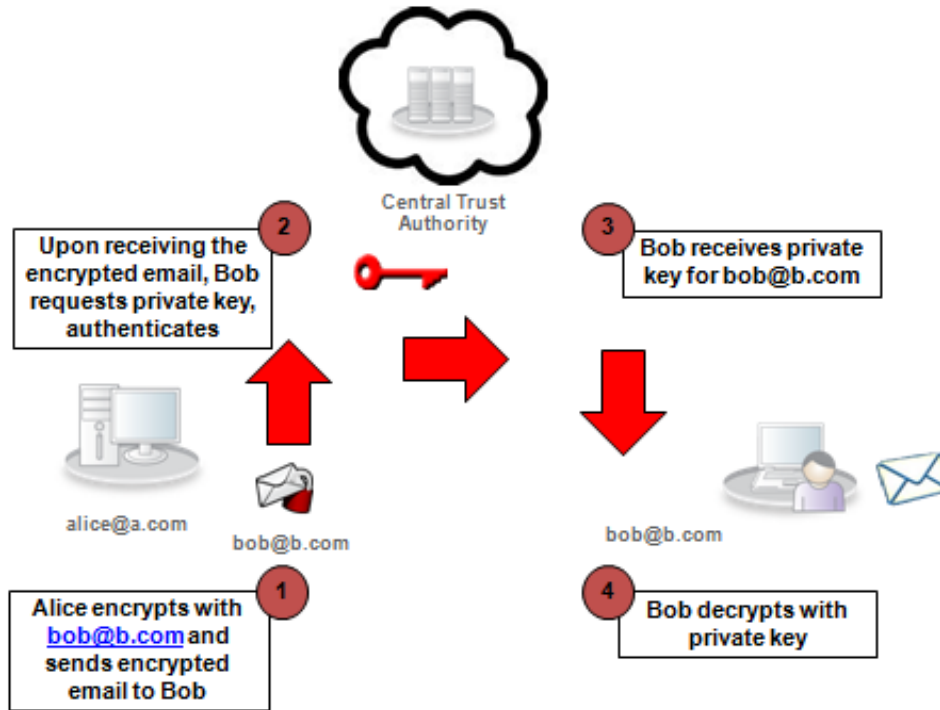
Trend Micro Encryption

Fortunately, a solution is available that marries the benefits of IBE with the ubiquity of the cloud. Trend Micro Encryption provides an integrated portfolio of e-mail encryption services based upon:

- **A cloud-based infrastructure.** This is what sets Trend Micro's IBE offering apart. Rather than rely on premises-based servers/appliances for key management, user registration, and e-mail storage (i.e., storage of a sensitive e-mail before a recipient sets up an account to receive the message), Trend Micro Encryption provides a much less burdensome alternative by hosting key services in the cloud (Trend Micro calls these cloud services the Central Trust Authority (CTA)). Trend Micro's investment ensures the highest level of security for these cloud services. Furthermore, since IBE uses the recipient's e-mail address as a public key, the Trend Micro e-mail encryption cloud never "sees" e-mail content in clear text. E-mails are encrypted using the receiver's public key from the recipient's desktop. Once a recipient registers on the Trend Micro site, he or she receives a private key and is thus the only person who can decrypt any sensitive e-mail. With these attributes, Trend Micro Encryption eliminates both key management and web-facing e-mail encryption registration, storage, and distribution tasks.
- **Client software.** Like other e-mail encryption products, Trend Micro Encryption offers e-mail encryption clients, enabling encryption on an end-to-end basis from sender to recipient. The difference is that Trend Micro's solution eliminates the hassles associated with digital certificate distribution and management. How? Since Trend Micro Encryption is based upon IBE, key pairs are calculated by using the sender's e-mail address and a random 256-bit number known only to Trend Micro. Rather than rotating certificates, Trend Micro simply changes the 256-bit multiplier on a monthly basis, re-calculates private key values, and then sends the new private keys securely to all registered users. This makes the Trend Micro Encryption client nearly invisible to users—all they have to know is whether they want to encrypt an e-mail or not.
- **On-premises virtual gateway appliances.** Trend Micro also provides a gateway appliance to encrypt e-mails based upon pre-set rules. Unlike other vendors, however, Trend Micro's gateway is delivered as a virtual appliance rather than a physical server. This eliminates hardware costs and can simplify the network architecture by running the Trend Micro virtual gateway along with multiple other IT infrastructure VMs on a single server. Seamless integration with gateway anti-malware, anti-spam solutions from any vendor, or Trend Micro's InterScan Messaging Security Virtual Appliance provide simplified security.
- **Hosted Email Encryption.** For enterprises adopting a SaaS strategy for protecting e-mail to avoid any additional hardware or software, Trend Micro Hosted Email Encryption is an add-on for [Hosted Email Security](#)—seamlessly integrated into a single, easy-to-manage solution.

All keys are stored in the cloud, eliminating the need for premises-based key management servers. As an example, when Alice creates an e-mail to a new user named Bob, the Trend Central Trust Authority (CTA) creates a key pair based upon Bob's e-mail address. The e-mail is then immediately encrypted from Alice's workstation and sent to Bob. Bob won't be able to read the e-mail since he hasn't registered an account and has no private key, but he still receives an e-mail with a link for him to access the CTA directly to set up an account. Bob is then free to register at his convenience with no pre-defined set-up is necessary. Upon registration, he is provided with a private key which enables him to then decrypt and view the e-mail using a web browser—no software to download (see Figure 1).

Figure 1. How Trend Micro IBE Works



Source: Enterprise Strategy Group, 2010.

The Trend Micro IBE Cost Advantage

The Trend Micro IBE solution is designed to streamline the e-mail encryption architecture, ease user registration, simplify business processes, and offload key management tasks to the cloud. This should make e-mail encryption much more attractive to reluctant organizations alone. Aside from these benefits, however, Trend Micro's IBE-based e-mail encryption solution can also deliver real financial benefits from the initial purchase through product deployment and ongoing operations. Based upon ESG's research, this savings can be significant; in ESG's cost model, the total cost of a typical PKI-based e-mail encryption solution cost is more than four times as much as a Trend Micro Encryption alternative.

ESG's model is based upon an enterprise of 1,000 users based in two different facilities. To calculate the potential savings, ESG considered the following parameters:

1. Server costs
2. E-mail encryption gateway hardware costs
3. Capital cost for software
4. Software client installation costs
5. Software (non-client) installation costs
6. User training courseware development
7. User training time costs
8. Help desk call cost
9. Capital cost for software maintenance and support (1 year)
10. Cost of IT operations/management/administration

These costs were based on the assumption that operational tasks were performed by a full-time IT employee (i.e., senior security/network administrator) with a salary of \$75,000 per year. ESG added a 30% premium to represent an employee's benefits; therefore all labor costs are based upon a "fully loaded" full-time employee cost of \$97,500.

ESG's E-mail Encryption Cost Model

The cost comparisons between a generic PKI-based e-mail encryption solution and Trend Micro Encryption IBE solution are broken down in the following sections.

Server Costs

PKI solutions tend to require multiple servers per site for each e-mail repository. Typically these servers are connected on a high-speed internal LAN to guarantee high performance. Alternatively, Trend Micro Encryption offloads key management to the cloud, thus there is no need for any on-site servers. ESG's conservative estimated cost for each server is \$7,500; therefore, a traditional PKI solution will require a \$30,000 upfront cost for four servers as compared to a \$0 investment for Trend Micro's cloud-based e-mail encryption.

E-mail Encryption Gateway Hardware Costs

Many large organizations are deploying e-mail encryption gateways that enforce privacy policies based upon data structure and pre-defined heuristics. Since gateway solutions are fairly mainstream, this cost was built in.

Many vendors offer proprietary hardware appliances only. ESG estimates that these appliances cost \$20,000, so a PKI solution across two sites would carry an encryption gateway hardware cost of \$40,000. In Trend Micro's case, it packages its gateway as a virtual appliance. Based upon ESG research, most enterprise organizations tend to run between five and ten virtual appliances on each physical server. To be conservative, the ESG e-mail encryption cost models assumes that the e-mail gateway will be one of seven VMs running on a physical server, therefore Trend Micro carries an e-mail encryption gateway hardware cost of:

$$\$7500 \text{ per server} \times 2 \text{ sites} / 7 \text{ VMs per server} = \$2,142.86$$

Capital Cost for Software

Simply stated, a PKI solution means purchasing software licenses for a number of components like key management software and a secure web-facing encrypted e-mail store for non-registered user. Many organizations claim that PKI software can cost twice as much as a Trend Micro Encryption solution alone. In spreading these costs across all users, ESG estimates that a PKI solution carries a cost of \$20 per user compared to \$10 for the Trend IBE offering. Thus, the software cost for a PKI solution is estimated at \$20,000 while Trend Micro comes in at \$10,000.

Software Maintenance Cost

ESG assigned a conservative 20% for software maintenance across both solutions. This means that PKI software maintenance would cost \$4,000 per year compared to \$2,000 for Trend Micro.

Software Client Installation Costs

In ESG's model, client software is installed on all 1,000 employee PCs and laptops. In interviews with security professionals, ESG consistently heard that a standard PKI client software installation was fairly straightforward, but it did require a bit of time for each workstation. On the other hand, Trend Micro users consistently stated that client installation was extremely straightforward.

While installation estimates are difficult, ESG calculates that each PKI client requires about 20 minutes to install, while Trend Micro Encryption clients take about 10 minutes each. Based upon these estimations, it takes 333 minutes to install 1,000 PKI clients and 167 minutes to install 1,000 Trend Micro clients. In the ESG model, a fully-loaded IT employee making \$97,500 carries a per-hour cost of roughly \$46.86 per hour, therefore the software client installation costs breakdown as follows:

$$\text{PKI: } 333 \text{ minutes to install } 1,000 \text{ clients} \times \$46.86 \text{ per hour} = \$15,625$$

$$\text{IBE: } 167 \text{ minutes to install } 1,000 \text{ clients} \times \$46.86 \text{ per hour} = \$7,812.50$$

Cost of E-mail Encryption Solution Installation

Aside from the client software, all of the backend infrastructure like key management servers, gateways, and web servers must be implemented. Furthermore, PKI solutions depend upon the distribution of client certificates to all 1,000 users.

ESG found a significant difference between PKI and the Trend IBE solution here. As stated previously, a PKI solution requires multiple servers and the process of setting up a PKI infrastructure is notoriously complex. In a Trend Micro e-mail encryption environment, much of this difficult infrastructure set up is subsumed by cloud services, making overall e-mail encryption deployment far simpler. ESG conservatively estimates that a PKI infrastructure will require 50% of an IT employee's time (i.e., four hours per day) for a period of 25 days (100 hours) while a Trend Micro IBE solution will require 50% of an IT employee's time for five days (20 hours). Thus, the cost to install an e-mail solution is approximately:

$$\text{PKI: } 80 \text{ hours} \times \$46.86 = \$4,687.50$$

$$\text{IBE: } 20 \text{ hours} \times \$46.86 = \$937.50$$

Cost of Developing User Training and Courseware

This is another area where there is a significant difference between alternative technologies. With regard to PKI, security professionals consistently talked about a significant amount of time and effort required to document e-mail encryption policies and how they relate to software functionality and operations. This is because of the PKI overhead—users have to be educated about certificates, key pairs, key security, etc. Based upon these discussions, ESG estimates that it would take a senior security administrator a full five days to develop training courseware and a training curriculum for presentation to all employees.

As expected, training requirements for an IBE solution like Trend Micro Encryption were far less cumbersome. ESG estimates that a seasoned security person could prepare the necessary courseware in a single day. Based upon these estimates, the cost for developing user training and courseware are:

$$\text{PKI: } 5 \text{ days} \times \$375 \text{ per day} = \$1,875$$

$$\text{IBE: } 1 \text{ days} \times \$375 \text{ per day} = \$375$$

Cost of User Training

ESG made several assumptions here. First, of the 1,000 employees, ESG assumes that 50 work in IT and don't need the same basic e-mail encryption training as others. ESG also assumed that the average salary across all 1,000 employees to be \$60,000 or \$78,000 fully loaded.

Once again, user interviews pointed to a significant difference between PKI and IBE solutions in terms of user training. Given the idiosyncrasies of PKI, ESG estimates that training for non-IT personnel will require a two-hour training class. Since Trend Micro IBE systems are far more transparent to users, training will require 30 minutes at most. Based upon these estimates, training costs come out to:

$$\text{PKI: } 2 \text{ hours} \times 950 \text{ employees} \times \$37.50 \text{ per hour} = \$71,250$$

$$\text{IBE: } .5 \text{ hours} \times 950 \text{ employees} \times \$37.50 \text{ per hour} = \$17,821.50$$

Help Desk Costs

Based upon IT industry data, an average help desk call costs somewhere between \$25 and \$75. ESG split the difference and used \$50 for its model.

Given the complexities of PKI, large organizations consistently report a profound spike in the number of help desk calls for the first few weeks—if not months—after installing an e-mail encryption solution. The duration of these calls is difficult to predict, so ESG simply estimated one help desk call for every three employees in a PKI implementation. This calculates to 317 calls (i.e., $950/3 = 216.67$). Enterprises using IBE solutions report much lower help desk call volume so ESG estimates one call per every 25 users for a total of 38 (i.e. $950/25 = 38$). With these estimates, help desk costs are:

$$\text{PKI: } 317 \text{ calls} \times \$50 \text{ per call} = \$15,833.33$$

$$\text{IBE: } 38 \text{ calls} \times \$50 \text{ per call} = \$1,900$$

IT Management and Operations Cost

With multiple servers and a PKI infrastructure to look after, a PKI-based solution requires a lot of tender loving care. ESG estimates that a senior security administrator will spend about 40% of his or her time focused on e-mail encryption tasks alone. On the other hand, an IBE solution like Trend Micro Encryption uses cloud-based services for IT infrastructure that is especially time-consuming to manage. ESG estimates that a security team member will spend no more than 10% of his or her time caring for the e-mail encryption infrastructure. Using the fully-loaded employee cost, a year’s worth of IT management and operations costs would be:

$$\text{PKI: } \$97,500 \text{ for a full-time security administration} \times 40\% \text{ of his/her time} = \$39,000$$

$$\text{IBE: } \$97,500 \text{ for a full-time security administrator} \times 10\% \text{ of his/her time} = \$9,750$$

All of these costs add up to a significant difference between a traditional PKI solution and Trend Micro Encryption. Based upon ESG’s estimates, the Trend Micro solution costs about 78% less than the PKI equivalent (see Table 1).

Table 1. PKI vs. Trend Micro Encryption IBE Cost Comparison

Cost Categories	Competitive PKI	Trend Micro IBE
Servers	\$30,000	\$0
E-mail encryption gateways	\$40,000	\$2142.86
Capital cost, software	\$20,000	\$10,000
Software maintenance cost	\$4,000	\$2,000
Software client installation	\$15,625	\$7,812.50
E-mail encryption solution installation	\$4,687.50	\$937.50
Development of user training and courseware	\$1,875	\$375
Cost of user training (lost wages)	\$71,250	\$17,812.50
Help desk costs	\$15,833.33	\$1,900
Ongoing management and operations	\$39,000	\$9,750
Total	\$242,270.83	\$52,730.36
Difference	459% of IBE solution	22% of PKI solution

Source: Enterprise Strategy Group, 2010.

Over the course of five years, the extra costs associated with management/operations and software maintenance/support alone are fairly significant—a PKI solution will cost about 3.7 times as much. Based upon ESG’s model, PKI operations and software maintenance will cost \$215,000 over five years while Trend Micro’s Encryption will run at \$58,750.

Other Cost Considerations

ESG's model is based upon "hard costs" with logical assumptions and estimates based upon user interviews. In assessing the cost differences between a PKI and Trend Micro Encryption, ESG also came across many "soft costs" that are more difficult to calculate. While these costs weren't built into the model, ESG believes that CIOs and CISOs should take them into account and assess how they might impact their particular operating environment and requirements. These costs include:

- **Business process changes.** Many organizations insist that e-mail encryption technology does not interfere with day-to-day business operations between partners, so IT has to go out of its way to make training, usage, and deployment as seamless as possible. One CISO reported that this process required about 25% of his time as well as one half of a full time employee for a month. As mentioned previously, IBE solutions like Trend Micro Encryption eliminate the bulk of this requirement.
- **New user set up time.** Each time an e-mail is sent to a new recipient, IT has to register the user, set up an account, ship him or her a certificate, and then maintain this account forever. This could represent significant operational overhead for growing e-mail encryption projects that touch numerous external organizations.
- **IT technical negotiations.** Organizations seeking to exchange encrypted e-mails must understand each other's e-mail environment, certificate authorities, and key management protocols. This will require meetings, planning, and possibly some type of technical integration. Obviously, projects like these can be costly.
- **Web-facing resources.** Encrypted e-mails to non-employees will most likely be stored in web-facing servers. These servers must be secured, maintained, and have adequate resources for a growing number of e-mails over time. Some of these costs are reflected in ESG's cost model, but others should be considered.
- **Liabilities.** What happens when an e-mail containing sensitive data is sent, but the recipient doesn't open it for weeks or months? Typically, the e-mail will remain on the web-facing gateway server. This can create a dicey situation over time as unread sensitive e-mails pile up. Should these be deleted? Retained? For how long? A PKI-based solution means that the CISO must evaluate these issues and discuss strategies with the legal department. Trend Micro Encryption avoids them all.
- **Encryption overhead.** Suppose one needs to send a sensitive attachment in an e-mail to 100 people, how is this operation executed? A PKI solution will use each recipient's public key to encrypt the whole enchilada and thus will end up encrypting the attachment 100 different times. With Trend Micro, the attachment will be encrypted once using a symmetric key and then the actual e-mail and the common symmetric key will be encrypted using the recipient's private key. This may seem like a subtle difference, but Trend Micro requires far fewer resources for execution and management. Organizations with bulk sensitive e-mail requirements should consider the hardware and operating cost ramifications.

The Bigger Truth

In the current environment of data breaches and sophisticated threats, CISOs should be taking every conceivable precaution to protect their organizations' data and IT assets. This means ubiquitous data encryption of sensitive data—at rest and in motion.

E-mail encryption certainly fits this category, so it should be used religiously. Yes, past problems with complex disruptive e-mail encryption technologies were very real and worth avoiding, but this is no longer the case. E-mail encryption solutions based upon IBE can be deployed across the enterprise without the historical headaches associated with PKI. It is time that this fact is recognized.

The benefits of IBE solutions like Trend Micro Encryption are obvious in theory: a simplified architecture, easier deployment, user transparency, and lower cost operations. ESG's cost model estimates that these benefits can result in a very real 78% cost savings over more cumbersome PKI alternatives. CISOs should use the model as a template for their own environments; change the number of seats, the cost of a full-time employee, and the software acquisition costs accordingly. Regardless of the inputs, the cost savings will be extremely apparent.

Finally, ESG understands that encryption can be a scary technology. Given this, what better reason than to outsource the bulk of the geeky security operations to an expert? Trend Micro Encryption's cloud-based architecture provides the confidentiality and integrity benefits of e-mail encryption without the technology headaches. This alone should make Trend Micro Encryption a top e-mail encryption choice for most organizations.



Enterprise Strategy Group | **Getting to the bigger truth.**