

TECHNOLOGY INSIDER ENCRYPTION

CLEAR CHOICE TEST E-MAIL ENCRYPTION

CipherTrust tops encryption field

BY TRAVIS BERKLEY, NETWORK WORLD LAB ALLIANCE

Encrypting e-mail is easier than you might think. We discovered this during a Clear Choice Test of six products that not only bolt onto your current e-mail system but also provide new features once you become encryption-savvy.

We cast a wide net to encryption vendors, and six accepted our invitation (CipherTrust IronMail, Entrust Entelligence, PGP Universal Series 500, PostX Secure E-mail, Tumbleweed MailGate and ZipLip Secure Messaging Suite). Voltage Security, Sigaba, Authentica and Zix declined. Centurion Soft's CenturionMail was tested, but the desktop encryption system didn't fit our test bed and methodology (see story at www.networkworld.com, DocFinder: 8427).

CipherTrust's IronMail wins the Clear Choice Award for solid performance, administration and policy enforcement. While the other five products tested are right on CipherTrust's heels, IronMail offers the best all-around package. However, the other products offer strong features and might be a better fit for your environment.

Getting off the ground

For the most part, the cost of encrypting e-mail isn't prohibiting companies from deploying it — it's the complexity that comes from managing encryption keys and

certificates. Trying to manage encryption at the desktop has often been difficult. The products we tested let you manage encryption at the gateway (aka policy-based gateway e-mail encryption). More important, the products make encryption transparent to end users.

While we used Exchange Server 2003, these products can be used with any e-mail system that uses SMTP. Outgoing e-mail is sent to a gateway server for processing. With inbound mail, the products process the mail first, decrypting if needed, and then forwarding results to the current e-mail system.

Including others

The next big question is what to do when e-mail recipients aren't using encryption. Fortunately, the vendors have addressed this problem with a Web-based interface that external recipients can use to retrieve encrypted e-mail. If the system cannot find a key to encrypt an outgoing message, it is moved to a Web site on the sender's net-

work. The system then sends a clear-text message to the original recipient, directing them to the Web site. When external users connect to the Web site for the first time, they are asked to create a password to log on. Once completed, users can log on and read the e-mail. The system is secured through a SSL Web browser connection.

Each product tested lets you control the content of the Web repository differently. Some let you delete messages automatically as they age and expire. PGP also lets you create a quota for message stores, which then bounces messages once the quota is reached. This is done because you are essentially hosting the e-mail for external recipients, and the sender should have some control over the resources committed to this effort.

All of the products we tested let you brand the Web site to some degree to look like your other corporate Web pages. The amount of branding varied greatly. On the less flexible end, PGP lets you load a logo and create a custom banner message. At the other extreme, CipherTrust allows complete branding of multiple Web interfaces. This is done to accommodate a company's branches or departments. The other products fell somewhere between these two extremes, offering flexibility in branding the Web interface to match a corporate image.

ZipLip and PostX offered an additional

NetResults E-MAIL ENCRYPTION

Product	IronMail 5.0.1	Universal 2.0 Series 500	MailGate Secure Messenger 6.1	Entrust Entelligence	SecureEmail v5.3	Secure Messaging 5.1.12
Vendor	CipherTrust	PGP	Tumbleweed	Entrust	PostX	ZipLip
Price	\$30,000 as tested	\$20,500 as tested for 500 seats, one-year subscription.	\$10,000 as tested	\$100,000 as tested (individually, appliances start at \$40,000 each).	\$15,000 as tested by subscription, or \$33,000 for perpetual licenses.	\$39,500 for 500 users.
Pros	Pre-configured for use, clean management interface, good policy engine.	Supports wide range of encryption ciphers and longer key lengths, very fast processing.	Good policy engine, Web site branding, good dashboard and management interface.	Good encryption options, good message performance, good policy engine.	Supports "secure envelope" alternative to Web delivery, good delivery performance.	Supports "secure push delivery" alternative to Web delivery, has user snap-in available.
Cons	Cannot do key harvesting.	Very minimal policy enforcement.	Lacks performance in delivery.	Management interface is complex, setup is tedious.	Not as much to offer as others in policy engine.	Modest messaging throughput, moderate policy engine in comparison.

way to deliver encrypted e-mail to external users without encryption of their own. E-mails can be sent as a JavaScript attachment, referred to as a secure envelope. When the first message is sent to an external user, a user must connect to the Web site and create a password. Once the password is registered and accepted, recipients can receive secure envelope messages. When one of these messages is received, the recipient opens the JavaScript attachment. The attachment asks for the password, and if correct the message is displayed. If you look at the source code of the message, you can see that it is stored in an encrypted format.

This method serves two purposes: It lets the message be stored on the recipient's mail system, instead of your own, and it also lets the recipient read the message while offline. However, this approach does rely on having a browser with good JavaScript support. Both systems worked well with Internet Explorer and Mozilla Firefox, but we had mixed results with the Konqueror and Safari browsers. Each product provided an explanation to the recipient if the browser couldn't execute the JavaScript.

Encrypt or not encrypt?

Figuring out what e-mail should be encrypted is best accomplished through policies. A policy is a set of rules that can be applied to each message, which then triggers an action.

Compared with the other products, PGP offered much less in this area. All of the PGP policies were based on e-mail addresses. We could group users together, create poli-

cies for specific domains and do some rudimentary subject-line scanning, but that was it. Actions included choosing the type of encryption to use or whether to send the message at all.

The other products could do these things, but offered additional features in how they scanned message content. ZipLip and Cipher Trust let us build dictionaries of words and phrases to scan for, and would trigger an action if these words were found in the subject line or message body. Entrust, PostX and Tumbleweed also let you type in regular expressions, a way of describing what the data might look like, rather than describing it exactly. For example, you might want to search for nine-digit numbers, which might or might not have dashes after the third and fifth digits (if you are looking for Social Security numbers). CipherTrust, Entrust and Tumbleweed are much stronger in this area than the others tested.

Compliance features are built into the products for companies governed by such legislation as the Sarbanes-Oxley Act or the Health Insurance Portability and Accountability Act. These products have

prebuilt lexicons that can be applied for these situations. The systems also have extra actions that deal with compliance requirements. Some include copying a message to a compliance officer, logging the message or blocking it altogether.

Keeping it secret

The core of the products we tested are the encryption keys and certificates. Each product tested used the Advanced Encryption Standard. Additionally, PostX can take advantage of the ARC4 algorithm, and ZipLip and Tumbleweed also use Triple-DES. Entrust and PGP offered the most flexibility in key generation, with support for five ciphers. What set PGP apart was its support of longer key lengths (up to 4,096 bits for Triple-DES), depending on the cipher. Generally, the longer the key is, the more difficult it is to crack. But this also means that it would take longer to encrypt and decrypt.

In our performance tests, PGP was the runaway winner. It chewed up our test loads significantly faster than the others. CipherTrust and Entrust finished second and third, with very similar results.

NETWORKWORLD CLEAR CHOICE							
The Breakdown	CipherTrust	PGP	Tumbleweed	Entrust	PostX	ZipLip	
External encryption 30%	3.5	4.5	3.5	4	3.5	3	
Policy enforcement 20%	4	2	4	4.5	3.5	3	
Administration/management 20%	4.5	4	4	2.5	3.5	3	
Performance 10%	4.5	5	3	4.5	4	3.5	
End-user experience 10%	4.5	4	4.5	3.5	4.5	4	
Installation/configuration 5%	5	4.5	4.5	3	4	3.5	
Documentation 5%	4	4.5	4	4	4.5	3.5	
Total score	4.1	3.9	3.8	3.8	3.7	3.2	

Scoring Key: 5: Exceptional; 4: Very good; 3: Average; 2: Below average; 1: Subpar or not available.



CipherTrust's IronMail appliance had solid performance, administration features and policy enforcement.

Care and feeding

All the products were managed through a Web interface, making administration easier.

PGP had the most compatible interface. On Internet Explorer, Firefox, Konqueror and Safari, it looked and performed the same. ZipLip, PostX, CipherTrust and Tumbleweed worked well with Explorer and Firefox, but didn't like Konqueror and Safari as much. Entrust worked consistently only with Explorer.

Additionally, Entrust was the only product that wasn't completely Web-based for administration. Its Policy Editor is a stand-alone application that runs on a Windows workstation. While the graphical application displays how the policy flows, it also requires you to download policy sets from the server, edit them and then upload them back to the server. The Entrust suite is also divided into three services: a compliance server, messaging server and Web mail delivery server. Each service has its own Web interface to manage. While they look similar, there were definite differences among them, including different password requirements. This made Entrust trickier to administer.

ZipLip gave us some quirky behavior — certain major configuration changes required us to restart our Tomcat application server. We couldn't restart through the Web interface; we needed to connect to the server and restart manually. Luckily, these major changes didn't happen frequently.

All products tested did well in showing a

summary-page dashboard view to quickly see how well the products were performing. CipherTrust, PGP, Tumbleweed and PostX have nice graphs on their dashboards.

All products included some reporting features. Entrust had the most in terms of number of reports that could be generated. ZipLip includes many predefined reports, but none were active by default. Tumbleweed also had several canned reports that could be executed from the Web interface or run on a schedule.

End-user friendly

While these products sit at the gateway, some products did have optional client components. Tumbleweed and CipherTrust include snap-ins for Outlook. These plug-ins add a toolbar button for the user, letting them request encryption for a message, whether or not the content triggers a policy. PostX has an optional client that pushes some additional functionality to the client. It also lets users force an encryption, as well as retrieve system keys and encrypt the message at the desktop. This lets the message travel in an encrypted state over an internal network.

PGP has an optional desktop client that integrates with its Universal Server gateway. We did not test it, because it is an add-on item. Among other things, users can manage their own encryption keys, which can also be sent to the gateway for proxy encryption. Further, there are tools included to encrypt local files on the client computer.

E-mail encryption delivery performance*

IN SECONDS

PGP	58
CipherTrust	125.6
Entrust	130.6
PostX	133
ZipLip	211
Tumbleweed	393.2

*Average time to trigger and deliver 1,000 encrypted e-mails, over five test runs.

Other transmission options

For recipients who have encryption on their end, the products offer additional features. For example, all of the products support Transport Layer Security (TLS). If you import the certificate of another company's e-mail server into your system, the two systems can establish an encrypted tunnel between the two sites to deliver the e-mail. Using TLS, the delivery of the message is encrypted, but the message itself is not.

Having the certificates imported into your system also let you do Secure Multi-purpose Internet Mail Extensions (S/MIME) encryption. This uses the same encryption key, but it encrypts the message itself, rather than just the connection. All products tested supported S/MIME, but Tumbleweed takes this a step further, embracing an emerging protocol called S/MIME Gateway, which helps automate the exchange of certificates. Additionally, CipherTrust, Entrust, PostX and, of course, PGP support PGP encryption as an alternative to S/MIME.

When messages are signed instead of encrypted, a message will be sent in clear text but allow for the message to be authenticated back to the stated sender to prove that the message hasn't been altered. Tumbleweed, Entrust, PGP and PostX can perform "key harvesting," which takes the public key from a digital signature and store

it for future use. When the system sees e-mail to that address, it can proxy-encrypt the message on behalf of that user.

Installation/documentation

CipherTrust's IronMail was the easiest to install. When you buy the system, you fill out a configuration worksheet. CipherTrust sends you the equipment preconfigured, and you simply mount the appliances in your racks, plug them in and turn them on. We were up and running with a base configuration in minutes.

Tumbleweed and Entrust also sent appliances. Also available as a software-only system, the Tumbleweed installation was painless. Once we mounted the hardware and attached to our network, a Tumbleweed engineer connects remotely to the system to configure it. The time was also used for a brief training session.

The Entrust installation was the most complicated. Each appliance included Red Hat Linux-based software preloaded, but

each piece had to be configured manually. We needed to run scripts, write down addresses and type them in later, which turned into busy work. Luckily, the Entrust documentation was very good, keeping us on track.

PGP sent us software that automatically installs on approved hardware, which included our HP ProLiant server. For customers who don't have hardware that meets the PGP specifications, the company also offers an appliance. The installation automatically formats drives, installs a Red Hat Linux kernel and sets up a base configuration with only a few questions to answer.

ZipLip and PostX were traditional software packages. While we installed both packages on Windows Server 2003, ZipLip also can run on Linux, and PostX can run on Linux, Sun or AIX systems. The PostX install was relatively straightforward, providing configuration options along the way. The ZipLip install was more involved mainly because



of the different configuration options available.

All vendors provided helpful documentation. We were most impressed with PostX, which gave us Quick Start guides that focused on specific functions. PGP gave us great configuration examples and a ton of screen shots. ZipLip provided a very good installation guide, but became thin after that. Other vendors provided a nice balance of installation and reference documentation.

All the products proved to us that getting started with e-mail encryption is much easier than you might think.

Berkley is the manager of LAN Support Services at the University of Kansas. He can be reached at berkley@ku.edu.

