NETWORKWORLD Reprint

THE CONNECTED ENTERPRISE ≡ MARCH 13, 2017

Zix wins 5-vendor email encryption shootout

Email encryption has come a long way since our last review

BY DAVID STROM, NETWORK WORLD

Email encryption products have made major strides since we last looked at them nearly two years ago. They have gotten easier to use and deploy, thanks to a combination of user interface and encryption key management improvements, and are at the point where encryption can almost be called effortless on the part of the end user.

Our biggest criticism in 2015 was that the products couldn't cover multiple use cases, such as when a user switches from reading emails on their smartphone to moving to a webmailer to composing messages on their Outlook desktop client. Fortunately, the products are all doing a better job handling multi-modal email.

In this review, we looked at five email encryption products, four of which employ encryption gateways and one that's end-to-end. The gateways usually rely on plug-ins to Outlook and browsers so you can continue using your existing email clients. The end-to-end product requires new clients for all encrypted message traffic.

The five vendors include two that we reviewed in 2015: HPE/Voltage Secure Email and Virtru Pro. The other three are Inky (the end-to-end product), Zix Gateway, and Symantec Email Security.cloud.

Winners and losers

The overall winner is Zix. It was easy to install and manage, well-documented, and the encryption features were numerous and solid. The only drawback was that Zix lacks a separate mobile client to compose messages, but having a very responsive mobile web app made up for most of this issue.

If you want a separate end-to-end product, you should look at Inky, which offers its own clients to support S/MIME encryption.

Voltage, Symantec and Virtru are also solid products, but are still behind Zix in terms of the flexibility of various encryption protocols used, along with DLP features that are built-in along with a simple and single pricing structure -- all things that Zix excels.

All of these encryption products will cost you a few dollars a month per user. While that doesn't sound like much, if you have an installation of several thousand users, the price tag could add up. However, the alternative is having your email stream available to anyone with a simple collection of tools that even teens can master.

Trends and bright spots

In 2015, we said that gateways may have fallen out of favor, but that trend has been reversed from what we could see from the current state of the art with these products. The gateways have gotten more capable for three reasons: they can better manage and eliminate any message residue that could be left on a local storage device, they make it easier for enterprises to manage message processing rules for compliance purposes, and they have auto-sensing mechanisms to deliver the best-effort encryption between the sender and recipient, so users don't have to figure this out on their own.

The biggest overall improvement in these products has been in better encryption key management. The difficulty associated with key management was made infamous last year with a Motherboard story where the reporter tried to get the inventor of Pretty Good Privacy (PGP), Phil Zimmerman, to exchange encrypted messages. Zimmerman sheepishly revealed that he was no longer using his own protocols, due to difficulties in getting a Mac client operational.

Since then, ProtonMail has improved its single-user free encryption tool (adding a Tor-capable version to further hide your email traffic) and Lavabit has relaunched its service (after closing its doors rather than give up its keys to law enforcement as part of the Snowden debacle.)

While these personal encryption products are improvements, there are also steps forward for the enterprise encryption email user. Some products, such as Zix, hide the encryption key process entirely from the user, so well that you might not even know that an encrypted message has passed from sender to recipient.

Others, such as Virtru and HPE/Voltage, use identity-based encryption management to verify a new recipient in their systems. Once a user new to these products clicks on a confirmation email, they are forever allowed access, their emails are automatically decrypted, and there is no need for any further effort to keep track of or to prove who you are.

That is the way all encrypted email products should operate if they are going to get used more often.

The second biggest improvement is the data loss prevention system (DLP) integration that Zix, Symantec and Virtru have as part of their products. Voltage also offers an extra-cost DLP option on top of the basic package. What this means is that all of these systems detect when sensitive information is about to be transmitted via email, and take steps to encrypt or otherwise protect the message in transit and how it will ultimately be consumed on the receiving end.

DLP has gone from something "nice to have" to more essential as part of business compliance and data leak hacks, both of which have increased its importance. Having this integration can be a big selling point of making the move to an encrypted email vendor, and we are glad to see this feature getting easier to use and to manage in these products.

A third improvement is the use of cloud-based services. All of the products tested offer cloud installations in their products, which make setup a breeze. Inky, Zix and Voltage also have on-premises servers, if that is more comfortable. Most of the products could be installed in about an hour, some even in minutes. This is a big change from earlier products that required lots of help from support staff to get up and running.

These are all great strides forward. But there are still a few issues, including the lack of support for Mac and Linux desktops. Most of the products offer a web-based alternative to reading and sending encrypted email on these endpoints, but only a few offer native clients or plug-ins for browsers or Outlook running on anything other than Windows.

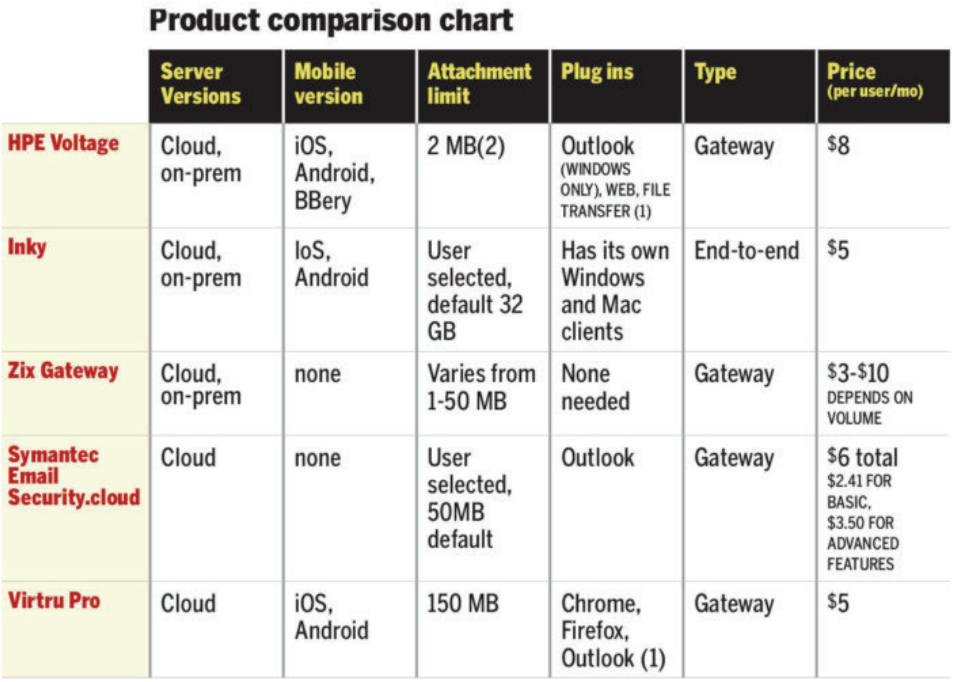
There are other potential gotchas contained in the fine print, such as limits on attachment size (shown in our summary table) or subtle configuration parameters that will require a call to the vendor's support line to complete the setup. We discuss those items in the individual reviews.

Frictionless encryption

In the past, encryption was frankly a pain in the neck. Users hated it, either because they had to manage their own encryption key stores or had to go through additional steps to encrypt and decrypt their message traffic.

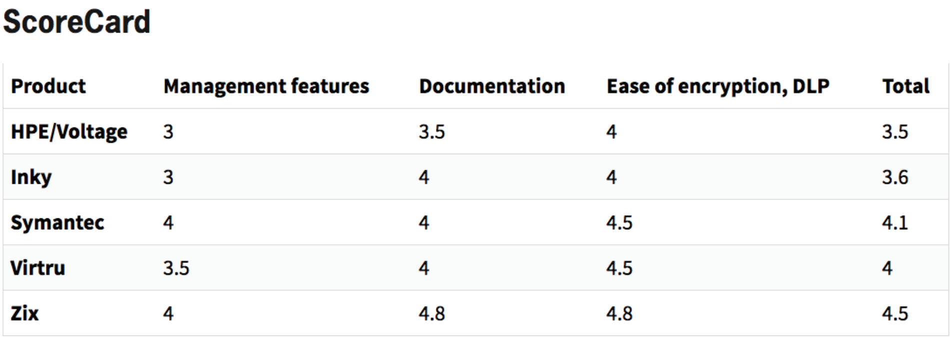
If a recipient wasn't using the same encryption provider, it was another painful process, which could quickly be multiplied by the number of different systems employed. We can see those days coming to an end, where encryption is almost completely frictionless.

So will that be enough to convince users to start using encryption for normal everyday emailing? We hope so. As the number of attacks and malware infections increase, enterprises need all the protection that they can muster and encrypting emails is a great place to start.



Product comparison chart

	Server Versions	Mobile version	Attachment limit	Plug ins	Type	Price (per user/mo)
HPE Voltage	Cloud, on-prem	iOS, Android, BBery	2 MB(2)	Outlook (WINDOWS ONLY), WEB, FILE TRANSFER (1)	Gateway	$8
Inky	Cloud, on-prem	IoS, Android	User selected, default 32 GB	Has its own Windows and Mac clients	End-to-end	$5
Zix Gateway	Cloud, on-prem	none	Varies from 1-50 MB	None needed	Gateway	$3-$10 DEPENDS ON VOLUME
Symantec Email Security.cloud	Cloud	none	User selected, 50MB default	Outlook	Gateway	$6 total $2.41 FOR BASIC, $3.50 FOR ADVANCED FEATURES
Virtru Pro	Cloud	iOS, Android	150 MB	Chrome, Firefox, Outlook (1)	Gateway	$5



ScoreCard

Product	Management features	Documentation	Ease of encryption, DLP	Total
HPE/Voltage	3	3.5	4	3.5
Inky	3	4	4	3.6
Symantec	4	4	4.5	4.1
Virtru	3.5	4	4.5	4
Zix	4	4.8	4.8	4.5

Zix Gateway: Frictionless encryption

Zix has been in the email encryption business for more than a decade, and its product shows. It is an interesting one to review because of how much it does under the covers, making the encryption happen in spite of what any end user is trying to do. This is one reason why they have so many large installations, and could be a reason why the software is so popular. Messages are sent and received without any specific user action, the encryption just happens. This makes Zix one of the most transparent and frictionless encryption products around.

Zix sells two products: the gateway that we tested, and an end-to-end encryption client that either works standalone or works with a Windows-only Outlook plugin to encrypt messages on the desktop before sending. The two systems don't interoperate. The gateway supports both Office 365 and Google cloud-based mailers. It can make use of OAuth to authenticate a user to both systems.

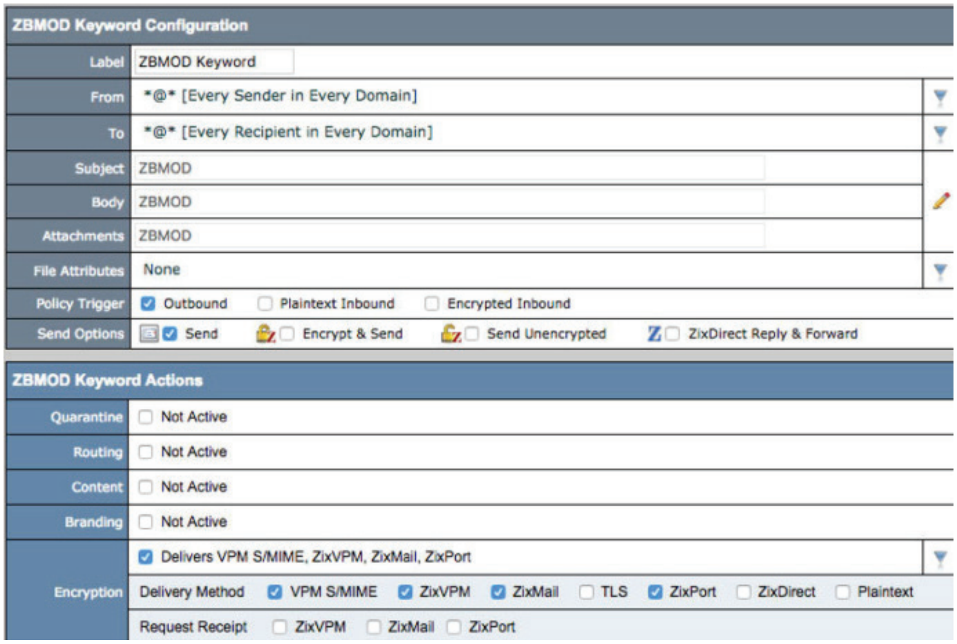
Getting the Zix Gateway installed will take a matter of hours, which can be reduced with personal support if you want it: it is included as part of the purchase price. Once set up, your employees might never know that their messages have been encrypted and decrypted, it basically operates under the covers and uses a variety of different techniques, depending on who is getting a message and how sensitive the contents. Unlike other products, such as Voltage that have added a "send secure" button, all mail is sent encrypted, if that is how you have set up your policies.

The idea is that Zix will encrypt a message whenever possible, as long as there's a secure pathway between the sender's and recipient's mail systems. You can configure your policies to do this, or to use one of its various secure protocols that are supported. Zix calls this "best method of delivery" and it is an important advantage and why you would want to choose it for your email provider. This means if you are sending email to another Zix customer, you don't have to do anything special to encrypt your message traffic. If recipients aren't Zix customers, their messages will be delivered using TLS protocols, or sending an encrypted HTML attachment (this last method is similar to how the other products work).

At the heart of the Zix encryption ecosystem is an innovative email DLP. This is included at no extra charge and perhaps one of the more important motivations for making use of their product. You set up content rules like in other DLP systems, but the rules are very easy to assemble, and you get a dozen or so pre-built ones to get you started that make things even easier.

All content is scanned including subject lines, message text and attached files. If the DLP engine finds a match with a policy rule, the mail is encrypted. If you use Outlook, you can also set the "confidential" flag in your message and that will trigger an encryption process.

The email DLP policies also show the power of the product. With some DLP



ZBMOD Keyword Configuration	
Label	ZBMOD Keyword
From	*@* [Every Sender in Every Domain]
To	*@* [Every Recipient in Every Domain]
Subject	ZBMOD
Body	ZBMOD
Attachments	ZBMOD
File Attributes	None
Policy Trigger	☑ Outbound □ Plaintext Inbound □ Encrypted Inbound
Send Options	☑ Send □ Encrypt & Send □ Send Unencrypted □ ZixDirect Reply & Forward

ZBMOD Keyword Actions	
Quarantine	□ Not Active
Routing	□ Not Active
Content	□ Not Active
Branding	□ Not Active
Encryption	☑ Delivers VPM S/MIME, ZixVPM, ZixMail, ZixPort
	Delivery Method ☑ VPM S/MIME ☑ ZixVPM ☑ ZixMail □ TLS ☑ ZixPort □ ZixDirect □ Plaintext
	Request Receipt □ ZixVPM □ ZixMail □ ZixPort

solutions, you have to worry about syntax, encryption certificates, or other plumbing issues. Zix takes care of all of that for you automatically. These rules are all click and set in a series of web screens that are very simple to navigate and the Zix support staff will help you assemble them if you can't figure them out. So for example you can create a rule that automatically encrypts any email that has a Social Security number or other personally-identifying information in it, or automatically encrypt a message with a particular recipient/sending combination.

You'll notice that there are no client pieces: you make use of your standard email clients. There is no additional software needed if you choose the gateway approach, since they handle the entire encryption and certificate processes. This also means no plug-ins, which is a nice touch.

One of the nice features is two separate training-based intranet sites (called User Awareness Programs). One is for customers, the other is for employees. Both walk you through the numerous features of the product. It is customized with your own landing pages and screen shots, and is well organized so a new staffer in your organization (or customer) can understand what Zix is doing in about 15 minutes.

Some other advantages: Zix maintains multiple data centers, including one in Europe if that is an issue for customers located there. Also, file attachment limits are set by the support staff from 1M to 50MB.

There are two big drawbacks to Zix. First it doesn't support sending messages from a smartphone. Like Symantec, there is no specific app that needs to be used, and all email needs to happen in the phone's browser. You either use a webmail client or respond to a message that you have sent from the Zix web portal. When you access the portal you can see its responsive design that takes into account the smaller browser real estate. The other use cases are all covered: end-to-end encryption with Outlook plug-in, gateway-to-gateway or gateway-to-supported email server.

The second issue is the various web portals that are needed to manage the product. There are many different parts to the product: the gateway code itself, which either runs in the cloud or can be installed as a physical appliance or a VM instance. There is a separate component, which handles quarantines, and a separate Web-based portal for messages that are sent to non-Zix users.

The gateway has a series of different web-based management screens: one for general operations, one for DLP management, one for reports about message traffic and one for handling quarantined messages. Each has its own URL, which means that is a lot of screens to visit, and to train your staff on. Obviously, they are working on consolidating and updating these into a more coherent package.

I had an issue with time-outs on my login screen to the overall web portal. Zix would lock me out during some but not all times when I returned to this screen. I couldn't recreate this and the company couldn't track this issue down. There is another issue, its reports lack any real flair and are fairly basic.

Pricing is one of the other advantages of Zix: everything is bundled in one simple all-inclusive price, depending on the number of individual senders that are licensed. This includes whatever server instance (cloud, VM, or appliance), whatever support is needed to get up and running, and minor ongoing support once your system is configured properly to your particular set of circumstances. Sample pricing is $3,500 per year for up to 25 senders, or $53,250 for up to 1,500 senders, based on a three-year commitment. This works out to about $3 a user a month for volume agreements. The one extra-cost option is the quarantine manager, which adds another $115 per year for up to 25 senders or $17,250 for up to 1,500.

How we tested email encryption

We used a combination of Mac and Windows 7 desktop clients, an iPhone and an Android tablet to run the various programs, using Safari and Chrome browsers. We set up several internet-based mail domains, and added plug-ins to Windows 7 machines running Outlook 2013 and any browsers to support the various email products' encryption features. In setting up this entire infrastructure, we looked at the following evaluation criteria:

1) Enterprise management and control features

These include how a product can recover from error conditions and how useful it is in troubleshooting email problems. We looked at how easy it was to set up new mailboxes or terminate existing ones. We also noted in the summary chart what the attachment size limits, if any, are specified by each vendor, how encryption keys are handled, and if any residue remains on endpoint devices.

2) Documentation

We looked at the user interfaces (Web, mobile and desktop clients) and how they differ and how they are documented or supported with online tutorials and help files.

3) Ease of encryption

Ease of use when it comes to applying encryption is now an important feature. This includes how to recover a lost password, how various endpoints encrypt and decrypt messages, and what DLP-like features are included.

zix®

www.zixcorp.com
866-257-4949
sales@zixcorp.com