Email Encryption powered by Zix™

Purpose-built to help businesses achieve cyber resilience

Benefits

- Enhanced security for business-critical communications
- Enhanced security status in regulated industries
- Single management console for multiple email security products
- Single vendor for cyber resilience solutions
- Secure Compose option allows any business partner or client outside of your organization to initiate an encrypted email into your organization through a Secure Messaging Portal
- Secure, bi-directional email
- User authentication for inbound email messages
- Customized drop-down list of company email addresses, names or departments

Challenge

Email is the most vulnerable aspect of your business and the easiest for employees to send sensitive information. With the rise of remote work, the need for secure email exchanges is greater than ever. Securing email is challenging for organizations of all sizes due to increasing threats and regulatory requirements. Data loss prevention (DLP) is also crucial, seeing as the rise of remote workers has also led to more data loss via email. Organizations need a turn-key solution is to secure email communications and prevent data leakage.

Solution: Email Encryption powered by Zix

Advanced Email Encryption (AEE) removes the hassle of encrypting email and gives teams the peace of mind that sensitive data sent via email is secure. Using advanced content filters, emails and attachments are scanned automatically and any message containing sensitive information is encrypted for delivery. AEE increases your threat defense and empowers everyone to communicate safely outside of your network. It automatically encrypts or quarantines based on policies you define for any email environment to secure your mailbox far beyond its native capabilities.

Advanced Email Encryption can also provide senders and managers insight into what caused an email to encrypt, helping to promote awareness of your email compliance policies. And if an unauthorized employee sends an email with sensitive content, Webroot can quarantine the message and alert management for review.

- Data Loss Prevention (DLP) filters trigger policies for encrypting, routing, blocking or quarantining email, work out-of-the-box and are highly customizable.
- Industry-specific policies detect information in email subject, body and attachments
- Help customers achieve governance, risk and compliance (GRC) best practices
- Policy-builder to select the right combination of filters for your customers' industry

Differentiators

- Multiple secure delivery options to fit your encryption needs
- Graphical reporting for compliance, delivery methods and more
- On demand and automatic encryption for sender and recipient
- Default and customizable email DLP filters included at no additional cost
- Empower external collaboration via Secure Compose portal

"With the alarming rate of identity theft in the United States, email encryption was crucial for the protection of our members' information."

Rifat Ikram,
Justice FCU's Vice President, Electronic Delivery and Support Services, Justice Federal Credit Union

How it works

Best Method of Delivery (BMOD)

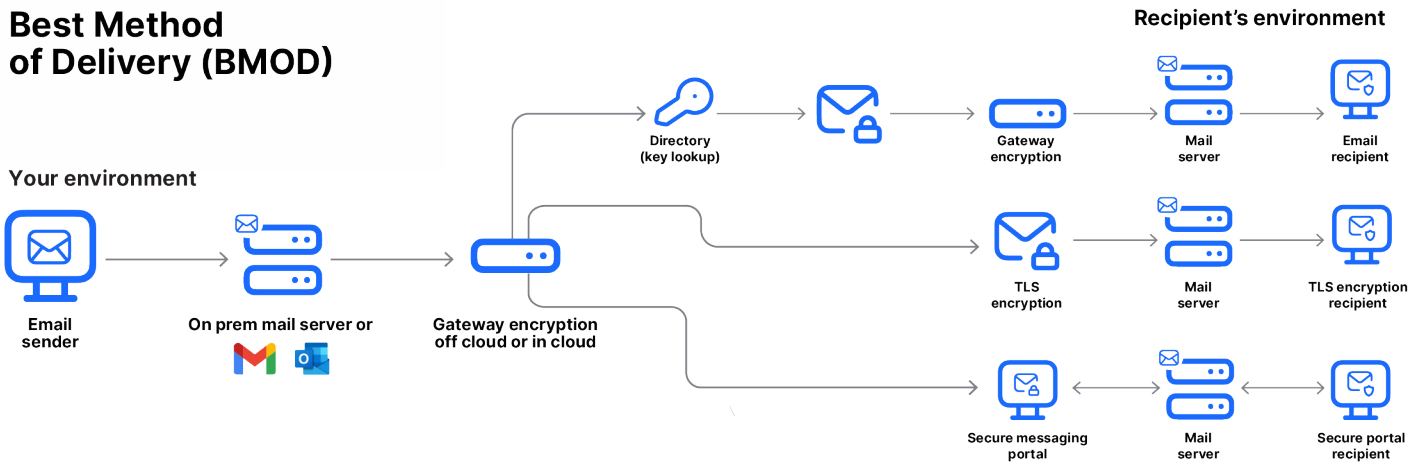
The multi-layer filtering engine delivers an extraordinary level of accuracy that reduces both false negatives (bad emails getting in) and false positives (good emails kept out). This reduces the time you spend managing the system and reduces friction for users.

Purpose-built to enhance your resilience against cyberattacks

OpenText Cybersecurity brings together best-in-class solutions to help your business achieve cyber resilience by enabling you to continue your business operations even when under attack. OpenText Cybersecurity can help you prevent and protect from breaches in the first place, minimize impact by quickly detecting and responding to a breach, then recovering the data quickly to reduce the impact and help you adapt and comply with changing regulatory requirements.

AEE is an integral part of our cyber resilience solutions and improves your security posture and provides the first line of defense by protecting and preventing the theft and leakage of sensitive data.

Best Method of Delivery (BMOD)



Delivery option 1

- Bi-directional, transparent, securely deliver between Zix customers
- Message level encryption (S/MIME)

Delivery option 2

- Policy based Transport Layer Security (TLS) delivery

Delivery option 3

- Secure Messaging Portal
- Secure delivery to any device anywhere anytime

Microtel Systems Corporation 804 254-2057
support@microtelsystems.com
411 E Franklin Street, Suite 600 Richmond, VA 23219