opentext™

OpenText Core Email Encryption

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.

84% of IT leaders said that remote work makes DLP more challenging

Solution: OpenText™ Core Email Encryption

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 triggered an email to encrypt, helping to promote awareness of your email compliance policies. And if an unauthorized employee sends an email with sensitive content, OpenText Core Email Encryption 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

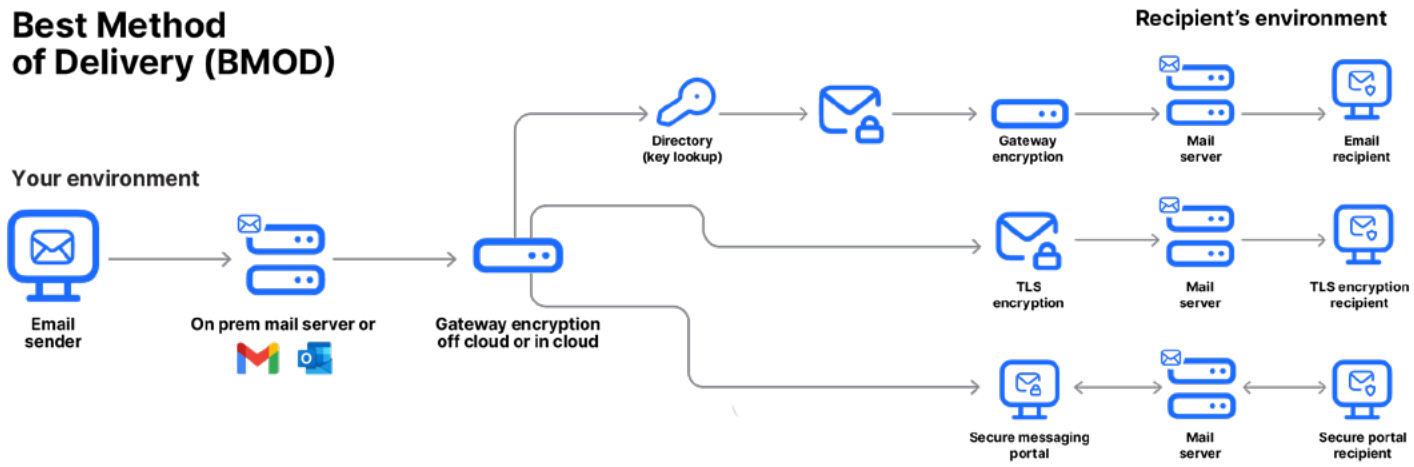
Best Method of Delivery (BMOD)

OpenText Core Email Encryption’s Best Method of Delivery (BMOD) scans outbound emails automatically, applying encryption based on customizable policies. This proactive approach reduces user errors, enhances security, and promotes compliance by quarantining unauthorized messages and alerting management for review. Employees are empowered to communicate safely outside your network without disrupting workflows.

The encryption is seamless and transparent, offering bi-directional protection with delivery options like message-level encryption (S/MIME), policy-based TLS, and a secure messaging portal for use on any device.

For over 20 years, OpenText’s Email Encryption has been trusted by industries such as healthcare, finance, and government, including 100% of US FFIEC regulators, the U.S. SEC, and 7 divisions of the U.S. Treasury. Its customizable policies and user-friendly portals enable businesses to safeguard communications effectively while simplifying email security management.

Best Method of Delivery (BMOD)



Delivery option 1

- Bi-directional, transparent, securely deliver between 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

Purpose-built to enhance your resilience against cyberattacks

OpenText Cybersecurity empowers businesses to achieve cyber resilience by enabling operations to continue during attacks. Our solutions help prevent breaches, minimize their impact with swift detection and response, and ensure rapid data recovery to maintain compliance with evolving regulations. AEE strengthens this resilience by safeguarding sensitive data against theft and leakage, providing a robust first line of defense.

Copyright © 2025 Open Text • 02.25 | 260-000342-003