opentext™ | Cybersecurity

DATASHEET

Webroot™ Advanced Email Encryption powered by Zix™

Purpose-built to help businesses achieve cyber resilience

Challenge

Email is the most vulnerable aspect of your business. It's quite easy for employees to send sensitive information through email. With remote work, the need for your customers and business partners to easily send you sensitive emails and files has never been greater. For businesses of all sizes, securing email communications is a challenge because of the ever-increasing threats via email. Also, regulatory requirements such as HIPAA, Sarbanes Oxley and GBLA mandate that sensitive and confidential data be protected because if it falls into the wrong hands it could result in reputational damage as well as huge financial loss due to fines from which businesses could possibly never recover.

In addition to data protection, businesses must keep an eye on data loss prevention (DLP) as well. The increase in the number of remote workers since the pandemic has led to an increase in data loss via email as well. According to Tessian, State of DLP 2020 (includes U.S. and the U.K.) survey, 84% of IT leaders said that remote works makes DLP more challenging. In summary, organizations need a solution that is easy to use, will secure email communications and prevent data leakage of sensitive information.

Solution: Advanced Email Encryption (AEE) powered by Zix

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. Webroot 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.

- Webroot 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

- Default and customizable email DLP filters included at no additional cost
- 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
- Empower external collaboration via Secure Compose portal

Key Benefits

- Enhanced security for business critical communications
- Enhanced security status in regulated industries
- Single management console for multiple email security products
- Deal with a single vendor for cyber resileince solutions

Secure Compose 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

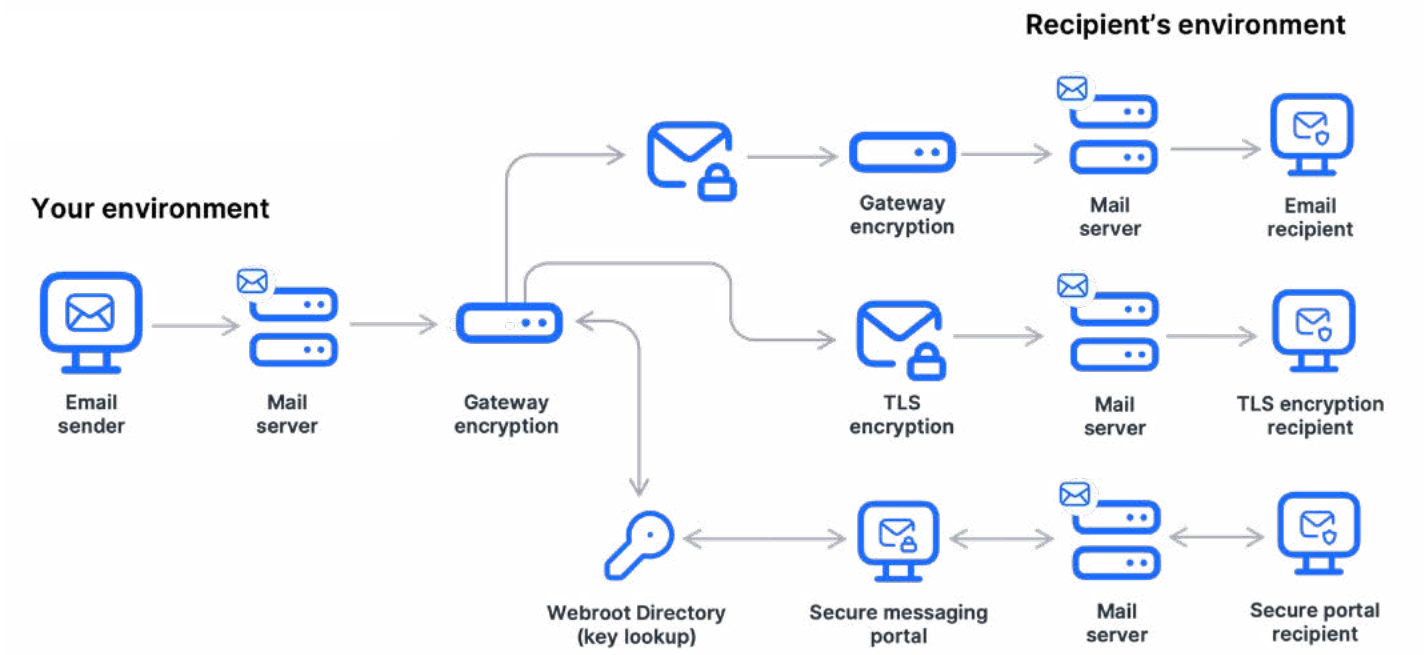
How it Works: Best Method of Delivery (BMOD)

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 Security Solutions 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. Together, Carbonite and Webroot 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.



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

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk. DS_053123