Email and Message Encryption Buyers Guide

Maintaining the integrity and trust of your brand, transactions, and customer workflows are both a business enabler and a regulatory mandate. For this reason, securing all email communication and collaboration is not an option but a requirement. Organizations must take a proactive approach to encryption given a single exposed record can result in heavy fines or a significant loss in customer trust. Further, a proactive, best-of-breed email encryption approach will make it easier to achieve your business objectives:

- **Aligning with Compliance and Privacy Regulations**
  According to Gartner, by 2022, 65% of the world's population will be covered by data privacy laws. With the constant expansion of regulations, it is critical that customers align with vendors who have worked with highly regulated organizations such as members of the Federal Financial Institutions Examination Council (FFEIC) and understand regulatory requirements such as the Gramm-Leach-Bliley Act (GLBA) and can help ensure that the technologies that are put in place ensure compliance.

- **Protecting the Corporate Brand and Customer Trust**
  Organizations that actively promote digital trust attract and retain 40% more customers than those that don't, says Gartner. Customers, partners, and employees are more likely to engage and maintain an open line of communication if they trust that the organization can protect their sensitive information. Organizations should work with vendors who have built a reputation of providing tools that are easy to use while enforcing the strictest forms of encryption to maintain that trust.

- **Preventing Data Leakage due to Compromised, Malicious, or Careless Users**
  While organizations conduct their best efforts to protecting their users from external threats and fostering a safe working environment sensitive information does unfortunately make it into to an email out of the organization. To safeguard confidential information when leaving your protected network, organizations must partner with vendors who deploy a holistic solution with the ability to accurately identify and protect sensitive information destined for an external recipient.

The right email encryption solution to meet today's regulatory and internal governance needs can be had but must deliver on the following critical requirements:

zix | appriver

Identification and Data Loss Prevention

The solution must provide visibility into the email message flow to allow organizations to adapt to the changing regulatory landscape and further understand what sensitive information must be protected or is unknowingly being used within the email flow. Finally, the solution must provide the remediation controls to appropriately investigate and remediate a policy violation related to your regulatory needs.

Requirement	Yes/No
Out-of-Box regulatory policies that identify data records related to but not limited the following: HIPAA, GLBA, PCI, SSN, FERPA, PII, GDPR, FINRA, etc.	
Customer defined policies that identify specific data records or a string of characters/words related to internal governance or email use policies	
Customer defined policies that identify message header or envelope details related to the sender, recipients, or X-headers	
Customer defined policies that identify message attribute details such as the attachment extensions, message size, or file triggers	
Ability for pre-defined policies to detect content with the Subject, Body, or Attachments within the message	
When policy is triggered, ability to enforce one or more policy actions: • Encrypt the Message • Quarantine the Message • Re-Route the Message to a different server or recipient • Delete the Message • Generate a Log • Notify the Administrator, Sender, or Recipient	
Ability to scan outbound messages for policy parameters	
Ability to define individual users or group managers to review DLP email violations	
Comment and auditing options to track remediation of a DLP policy violation via the quarantine manager	
Highlights the exact content within the message that triggered the DLP policy	
Ability to allow sender or recipient access to release messages that triggered a DLP policy	
Ability for designated reviewers to notify the sender, recipient or other personnel of the policy violation	
Ability for designated reviewers to delete a quarantined message or release the message to its original recipients	

End-User Experience and Access

The solution must provide a frictionless experience to ensure that the end-user's productivity is not impacted and that broad adoption of the solution is accepted to maximize the protection of your critical information.

Requirement	Yes/No
Automatic, non-user initiated encryption based on DLP or customer defined policy trigger	
User initiated encryption via an inserted Keyword(s) within subject, X-header, or body of the message	
User initiated encryption via a Microsoft Outlook Add-in	
Transparent Delivery via a Secure Message Encryption Network: Zix-to-Zix requires no user intervention to encrypt messages with other Zix Encryption users. Message is encrypted at the sender's gateway and decrypted automatically at the recipient's gateway.	
Transparent Delivery via policy-based TLS with customer-defined authentication and encryption levels.	
End-to-End Encryption from sender's desktop to recipient's desktop	
No client install required to view an encrypted message	
Support for International languages e.g. German, French, Spanish, Portuguese etc.	
Multiple delivery options per message and recipient: SMIME, secure desktop, TLS, Secure PDF, Secure Push, and OpenPGP	
Automated ability to detect supported encryption method type for each message recipient via a Best Method of Delivery (BMOD) architecture	
Ability to receive, view, and respond to encrypted email via a mobile device	
Ability to compose an encrypted email, reply, reply-all, or forward via a web-based Secure Messaging Portal	
Support for the customer's clients or partners to compose an encrypted email via the Secure Messaging Portal	
Ability to brand the Secure Messaging Portal for each supported business domain	
Secure Message Portal option with complete email client experience including contacts, drafts, and sent folders	
Support for encrypted push delivery option, whereby the entire encrypted message is sent as an HTML attachment, decrypted only via a password, and displayed in an Internet browser.	

Deployment, Security, and Integration

The solution must meet the demands of organization of all sizes from small business to very large enterprises. Customers must be able to trust that their information is fully protected in accordance with industry accepted regulatory requirements while at the same time ensure that the system is available to allow employees, partners, or end-customer to communicate at anytime from anywhere.

Requirement	Yes/No
Dedicated hosting or hybrid environment	
Certifications and Accreditations: • PCI DSS 3.2 • SOC2 and SOC2 for HiTrust • ISO 27001 • FISMA NIST 800-53 (moderate level)	
Automated 3072-bit S/MIME customer keys generation	
Centralized management of all customer X.509 certificates	
256-bit AES session keys to secure message communications	
Support for large amounts of daily transactions, with capacity to increase	
Proven 99.99% reliability and uptime	
Support for 3rd party DLP and Classification Systems	
Support for large attachment file send default 50MB (customer mail server configuration setting) with increases to 100GB via Secure File Sharing	
Integration with Advanced Email Threat Prevention with the ability to scan for threats prior to message encryption	
Secure Messaging Portal support for Single Sign On via SAML 2.0, OAUTH, and website integration via iFrames	

Administrative Controls and Reporting

The solutions must provide the necessary administrative controls to customize the environment for the organization's needs or be able to quickly investigate and remediate any issues with email delivery. Finally, administrators need to report the right insights and provide the right visibility to ensuring that the system is functioning as intended.

Requirement	Yes/No
Enforce encryption based on organization domain, department, or individual	
Support for role-based access	
Message search options to allows the ability to identify any message that has passed through the system	
Complete audit and reporting options detect user login, configuration changes, and message access activity	
Out-of-box reports include but not limited to: • Status of inbound and/or outbound message delivery • Method of email delivery • Method of encryption type enforced • DLP or Content policy triggered	
Free form text search to search within reports	
Ability to run ad-hoc or scheduled reports	
Ability to track message transactions for irrefutable, time-stamped Transaction Certificate and Certified Receipts	

Implementation and Customer Care

Organizations must work with vendors that not only provide a solution that will work once deployed but also sets the organization up for success during onboarding, implementation, and ongoing support. Organizations must demand high quality customer care and be able to trust that the vendor is looking out for the customer's best interest and not their own.

Requirement	Yes/No
White-glove installation support included with the service	
Advanced content filter customization included with service	
Live 24/7 US-based online and live support	
User training for encryption guidelines with screenshots and easy-to-navigate instructions (end-customer and employee facing documents)	

Conclusion

Zix has been the gold standard for email encryption supporting the Industry's largest email encryption network in the world. Zix is not only committed to providing a superior encryption solution that adheres to the strictest regulatory requirements but is focused on providing all the tools to mitigate the most serious complex cyber risks. The Secure Cloud ensures regulatory compliance through best-in-class email encryption, easy-to-use secure content sharing, advanced email threat protection and business communications archiving (email, instant message, and social media). Plus, it's all backed by Phenomenal Care for customers and 24/7/365 support.