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.

I

threats and fostering a safe working environment sensitive information does unfortunately make it into to an email out of the organization. To safegua rd 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:

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, FI Fnon emáu3s F th	

t)-3fi8 404.2 Tw 6.929 0 Tdd1.2 (s)0.149 0.18h0.271 rg0 -1.355 TD[(t)4 (h)-0.8cs3DC 26480.213 0 (del)-1p)-1.7 (o)0.8 (lic)4.5 (ie)1.6 187

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.	

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	

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