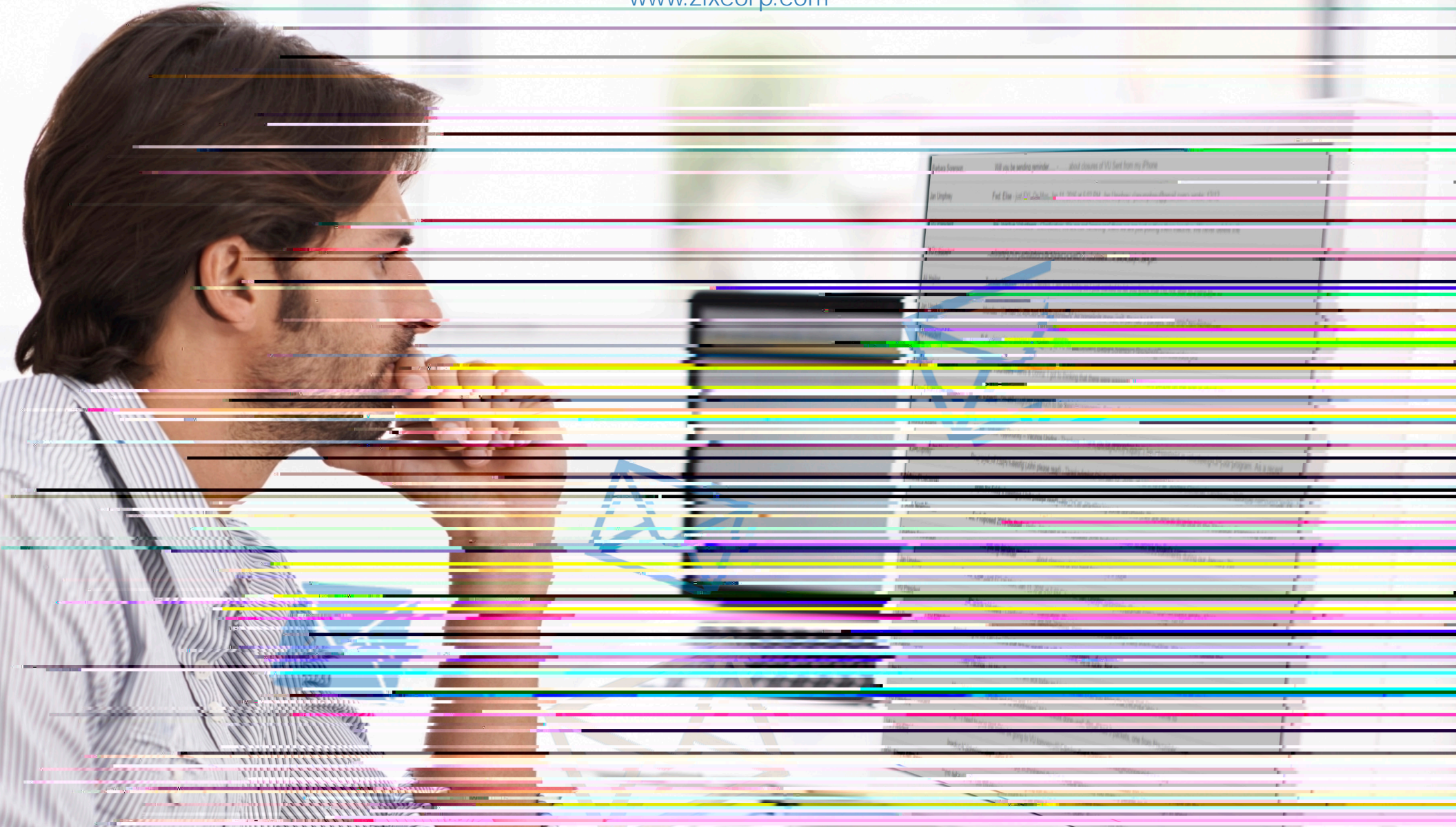


# Navigating Email Security

A Review of Email Encryption, Data Loss Prevention  
and How They Protect Your Business

[www.zixcorp.com](http://www.zixcorp.com)



The amount of sensitive information managed by business is immeasurable. Proprietary data, intellectual property, personal data collected from employees, former employees and job applicants, financial information provided for customer or patient payments – all create a treasure trove of data, and IT has the seemingly insurmountable challenge of securing it without impeding daily work and communication.

## Protecting the Most Used Communication Tool

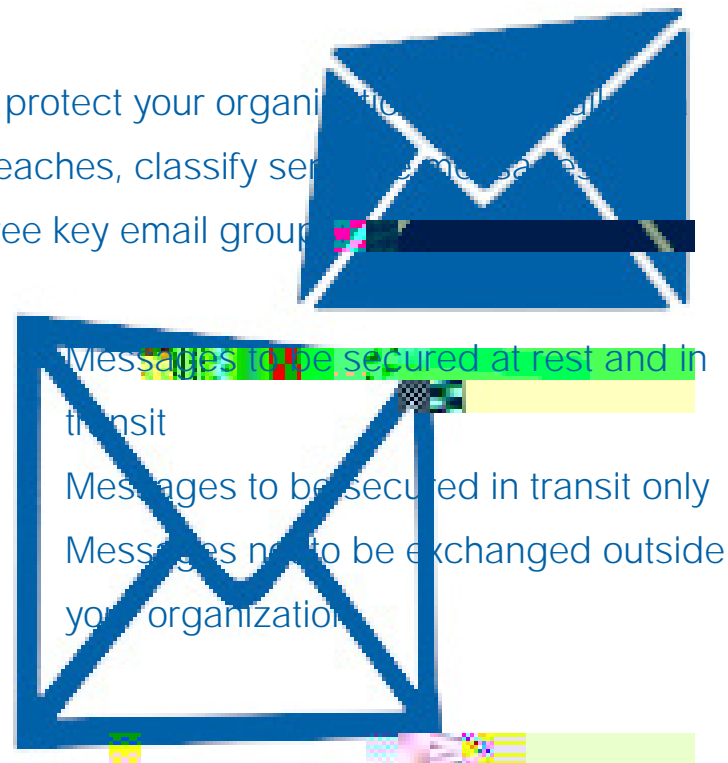
Despite the popularity of social media and instant messaging, email persists as the top communication tool for business.

To protect your organization from email data breaches, it's critical to classify sensitive messages into three key email groups.

1. Sensitive email secured at rest and in transit
2. Sensitive email secured in transit only
3. Sensitive email not to be exchanged outside your organization

By managing email in this manner, your organization will invoke the appropriate security – encryption or data loss prevention (DLP) – to enable or stop the exchange of sensitive information.

To protect your organization from email data breaches, classify sensitive messages into three key email groups:

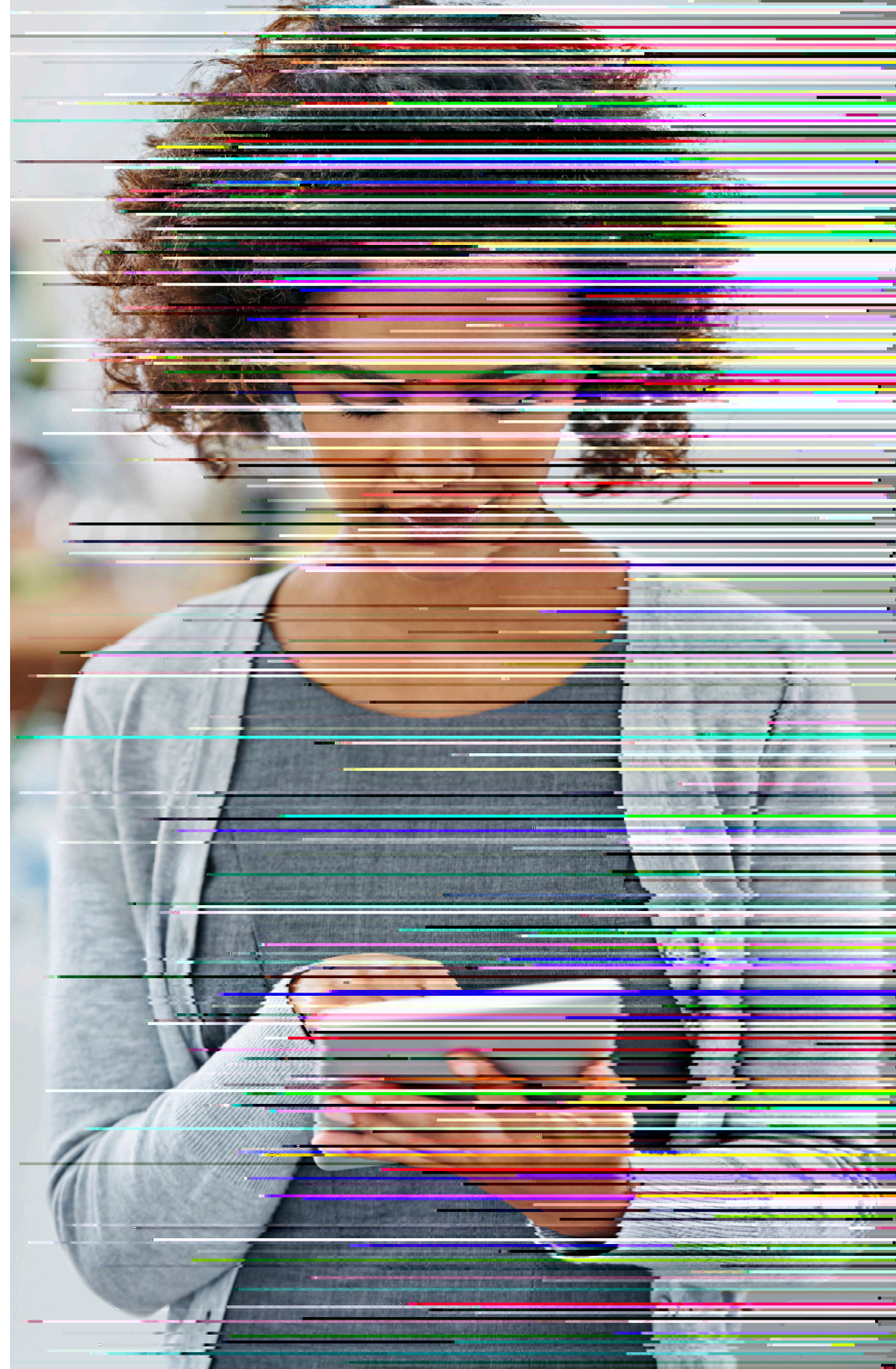


## 1. Messages to Be Secured at Rest and in Transit

End-to-end encryption safeguards email so that unauthorized individuals within and outside the organization's network are unable to read messages and any attachments. When email needs to be protected, the sender uses an encryption key to secure the message. For a recipient to view the message and

End-to-end encryption also offers a layer of protection against malicious threats outside your organization, known as advanced persistent threats. Despite even the greatest investment in network security and the most attentive IT department, there is no security barrier that is 100% foolproof against hackers attempting to gain access to your organization's network. Organizations can use end-to-end encryption to prevent outside, unauthorized individuals from stealing content in the most sensitive emails if they break through network security.

With security a high priority, the use of end-to-end encryption for all emails may be tempting, but its drawbacks shine light on another encryption method.



## 2. Messages to Be Secured in Transit Only

The beauty of email is its ease of use. The exchange of communication and attachments is seamless with employees, customers and partner organizations. By forcing senders and recipients to use a key to encrypt and decrypt every message, the convenience of email is lost, and the widespread adoption of email encryption is too cumbersome to succeed.

In using encryption in transit, your institution can take advantage of innovative solutions that not only secure email if it's intercepted over the public Internet but do so without requiring any extra steps from senders or recipients. Encryption and decryption happen automatically, keeping daily work flowing and allowing your organization to protect email as it travels outside your network.





Another benefit of encryption in transit is the convenience of maintaining security. While large, public breaches at Premera BlueCross BlueShield, Penn State University and the U.S. Office of Personnel Management did not involve email, the vulnerability exploited in those breaches was the result of missed security patches. With all the responsibilities IT departments hold, it's difficult for patches to be completed in a timely fashion.

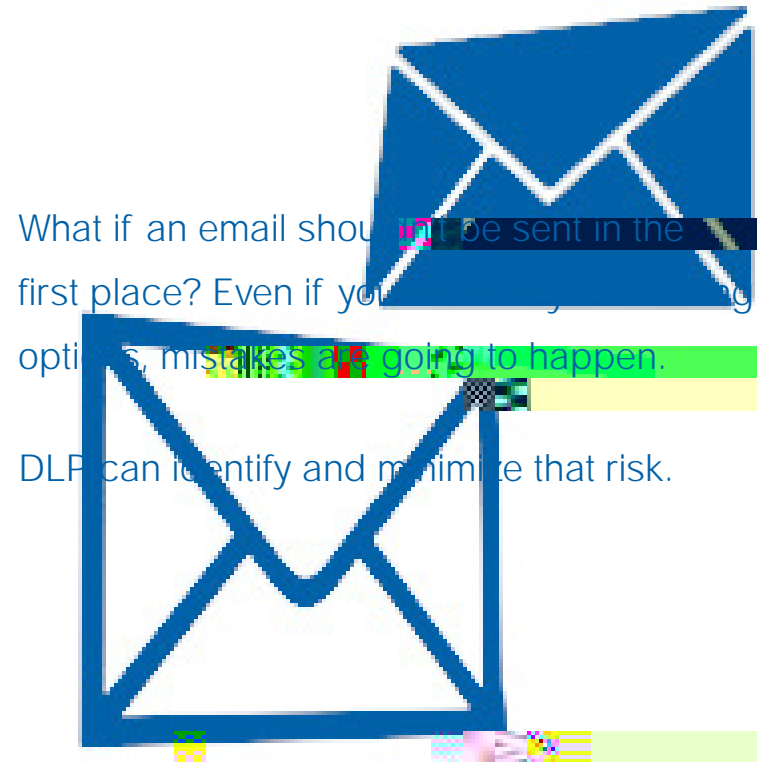
Unlike end-to-end encryption which requires installation and maintenance on each desktop, solutions for encryption in

### 3. Messages Not to Be Exchanged Outside Your Network

Email encryption can be used to protect sensitive data at rest and in transit, but what if email shouldn't be sent in the first place? Even if you exhaust your training options, mistakes are going to happen. DLP can identify and minimize that risk. More importantly, it can protect your organization from associated costs – fraud protection, regulatory fines and potential civil lawsuits.

In the past, DLP has been known for its costly, long implementation timelines. By focusing on the most used communication tool – email – and using a single application solution, IT can decrease the cost dramatically, reduce the deployment timeline from months to hours and rollout security with minimal impact on IT staff.

The solution scans all outbound email prior to leaving your institution's network using standard policy filters, such as HIPAA or Social Security number, or custom policy filters. If a policy is triggered, the email is sent to a quarantine system, where IT or the sender's manager can release the email or notify the sender that it cannot be exchanged.





## Balancing Needs with Different Security