Wake up and Smell the Breach: Protecting Your Email with Zix and IT Resource

Adam Lipkowitz, Sr. Account Executive, Zix

Gary Lutz, President, IT Resource


IT
Resource
PUTTING
IT ALL
TOGETHER
616.837.6930
www.itrw.net

About IT Resource

"Our goal is to provide the most comprehensive and cost effective IT solutions, and keep our customers happy with outstanding service."

Zix® PREMIER PARTNER

- Founded in 2000, IT Resource, Inc. is an enterprise-level information technology solution provider and managed services company
- Locations in Michigan and Florida
- Clients in over a dozen states & three countries
- Clients in Public Sector, Financial, Healthcare, Education, Legal, Manufacturing, Service, and others

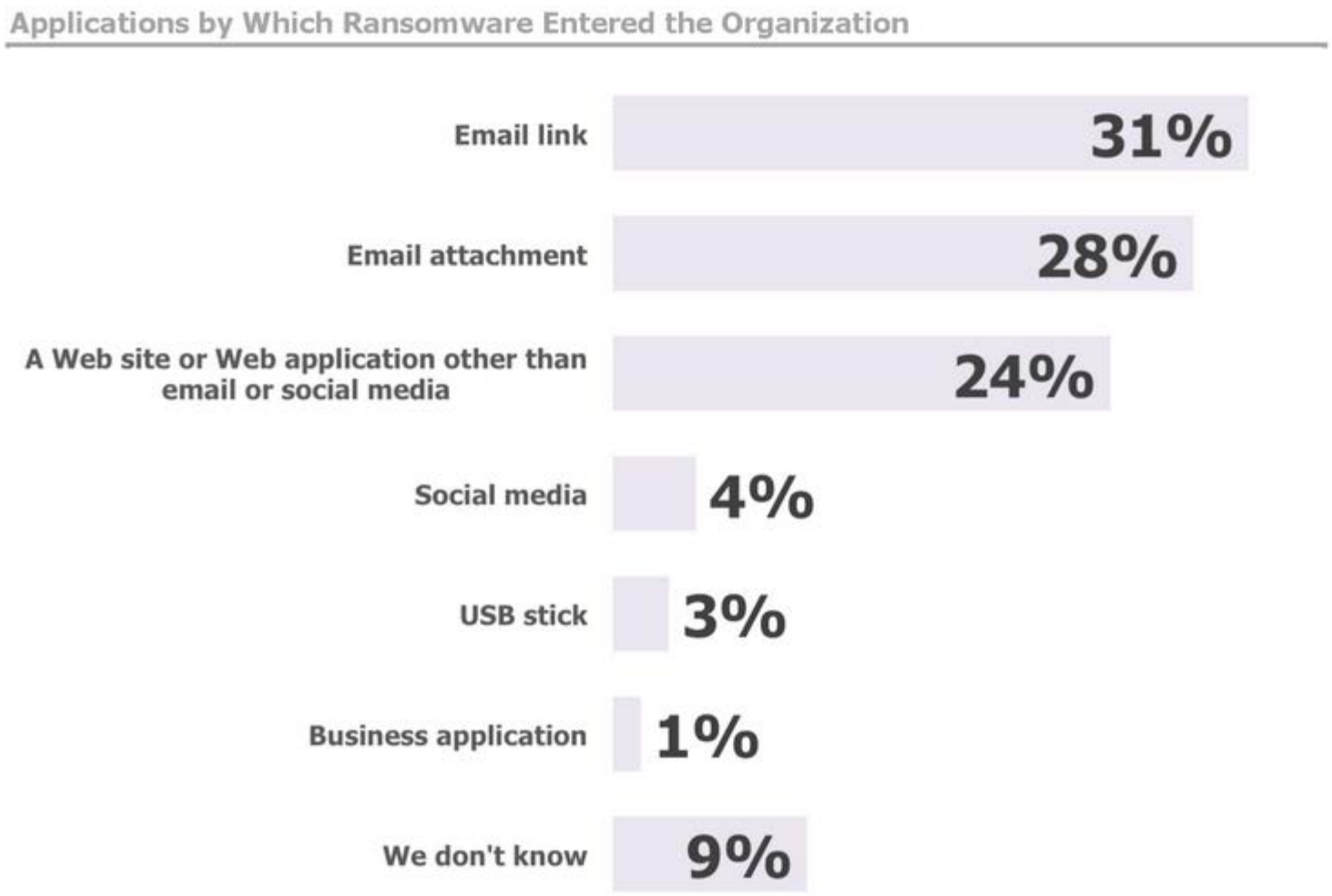
Our Core Values

Integrity – Honesty – Respect – Commitment – Collaboration - Innovation

WannaCry

- Attack started on Friday, May 12th and within one day had infected more than 230,000 computers in over 150 countries
- Using a vulnerability in Microsoft's Server Message Block (SMB) protocol, it installs a backdoor that transfers and runs the WannaCry ransomware
  - On March 14, 2017 Microsoft had released a patch for the SMB vulnerability
- After encrypting the files, it displays a "ransom note" informing the user they must pay $300 in bitcoins
- It also includes a "transport" mechanism that automatically scans for vulnerable systems and spreads itself
- The initial attack was unintentionally stopped by a security researcher that registered a domain found in the malware
- Within four days of the initial outbreak most organizations had applied updates, and new infections had slowed to a trickle

Ransomware in email



Source: Osterman Research, Inc.

Ransomware Statistics

- Phishing email attachments have become the #1 delivery vehicle
  - 93% of all phishing emails contain ransomware
  - In most cases the attachment is a Microsoft Office document
- Ransomware-infected email expanded 6,000 percent as compared to 2016
- Ransomware attacks quadrupled in 2016, with an average of 4,000 attacks per day
- Ransomware is on pace to be a $1 billion dollar source of income this year

Locky

2016 Ransomware

- Delivered as an email that had an alleged invoice requiring payment
- Attachment was a Microsoft Word document containing malicious macros
- When the user opens the document, it appears to be full of garbage, and had the phrase "Enable macro if data encoding is incorrect"
- If the user enables macros, malicious code was downloaded and executed to encrypt all files that match particular extensions
- A message displayed on the user's desktop instructs them to download the Tor browser and visit a specific criminal-operated website
- Website contained instructions for payment of between 0.5 and 1 bitcoin
- Since Locky was released there have been numerous variants released

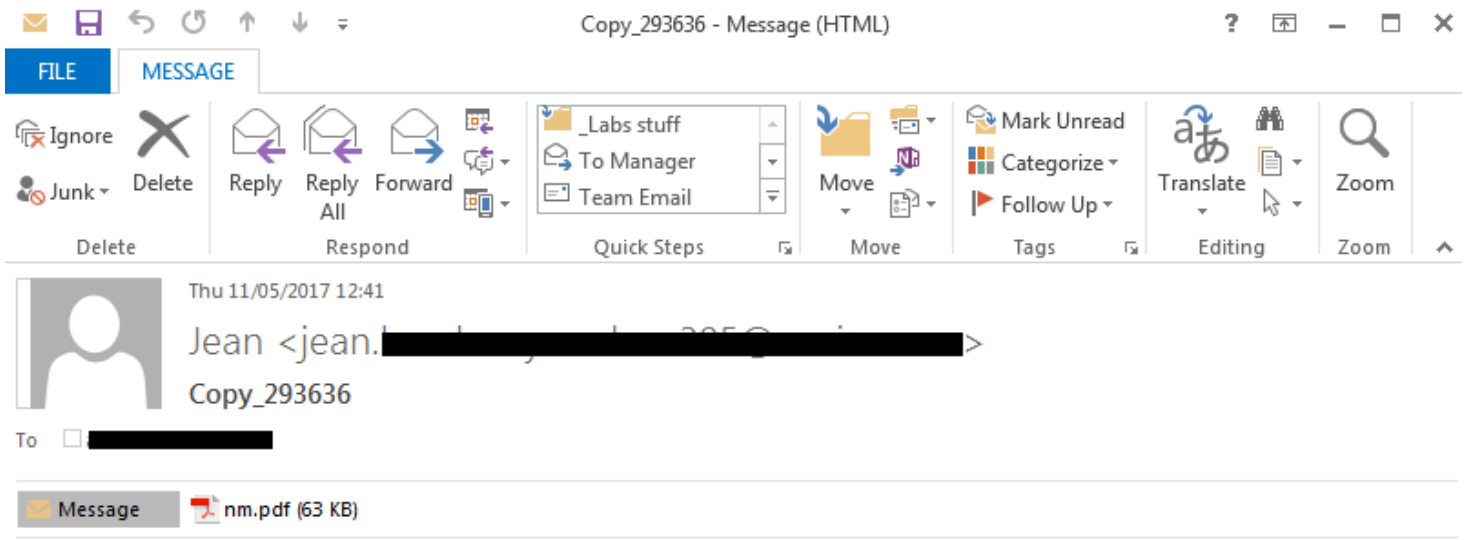
Ransomware Example

Jaff

- Emerges just one day before WannaCry
- Uses the Necurs botnet to send millions of emails from zombie endpoints
- Estimated 5 million emails an hour sent at peak
- Contained various subject lines regarding a receipt, scanned document, or report attached
- Email body was either blank or contained a brief note to print
- Attached file contained a Word document with Macro that when opened deliver ransomware
- Ransom of 2 bitcoin (approximately $5,500)

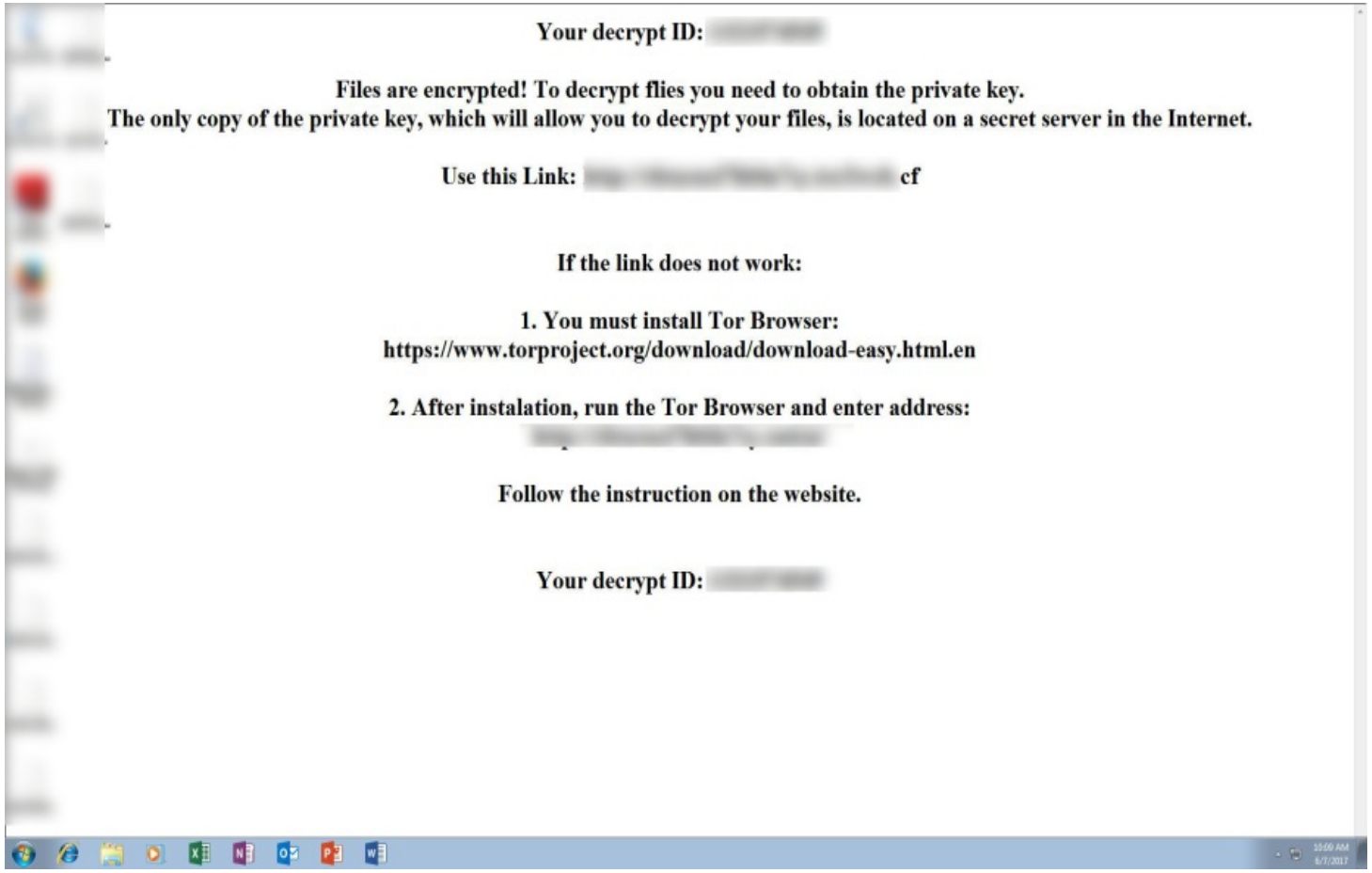
Ransomware Example

Jaff



Ransomware Example

Jaff



Ransomware

Bottom Line

- Most ransomware is delivered via email
  - Phishing attacks work
- Training alone will not work
  - Some users will still click
- Multi-layered filtering is required to identify attacks
  - IP blacklisting only will not stop attacks
- Must be able to detect zero-day ransomware
  - The attacks are always changing

An email security company focused on protecting business communication for our customers and their communities.

zix®

A Full Suite of Email Security

Email Encryption

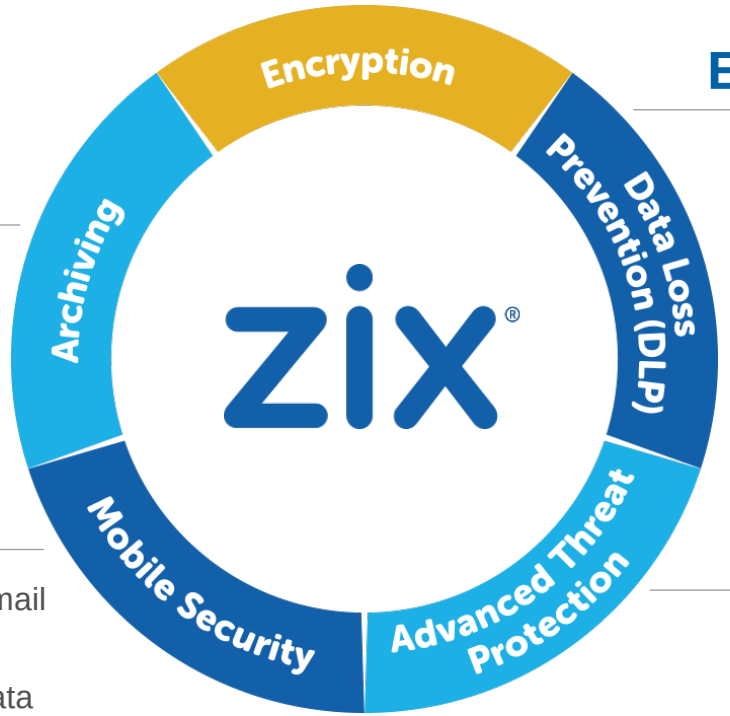
- Industry-leading email encryption solution
- Robust and scalable solution for organizations of all sizes
- Encrypts and securely delivers more than 1.4M emails daily

Email Archive

- Unlimited email storage for business legal compliance
- E-discovery search and hold

Email Mobile Security

- Provides employees with easy access to email while never storing data on the device
- Allows organizations to secure corporate data and meet compliance requirements



Email Data Loss Prevention

- Addresses the greatest source of data loss — corporate email
- Prevent improper exposure of sensitive information outside the network
- Significantly decreases complexity, cost, and deployment time

Email Threat Protection

- Defend against spam, viruses, zero-day malware, ransomware and phishing
- Multi-layered approach delivers 99.5% accuracy
- 30-day business continuity for disaster recovery

Email Threat Protection

Protecting Your Users

zix®

Email Threats

Understand the risk

- 65% of all email is spam
- 78% of people that claim to be aware of the risks of unknown links in emails will still click anyway
- 13% of people tested clicked on phishing attachments
- In Q3 2016 alone, 18 million new malware samples were captured
  - An average of 200,000 per day
- More than 4,000 ransomware attacks have occurred every day since the beginning of 2016
  - A 300% increase over 2015

Email Threat Protection

Accurate filtering, strong protection

Zix utilizes a multi-layered filtering approach that protects against spam, viruses, zero-day malware, ransomware and phishing.

- **Easy to implement and manage**

  Pre-configured filters require no setup or tuning

- **Highly accurate filters**

  Lets legitimate emails through while stopping attacks

- **Business continuity for emergency recovery**

  Users can access email through web interface

zix IT Resource

Email Threat Protection

Protect users from unwanted emails

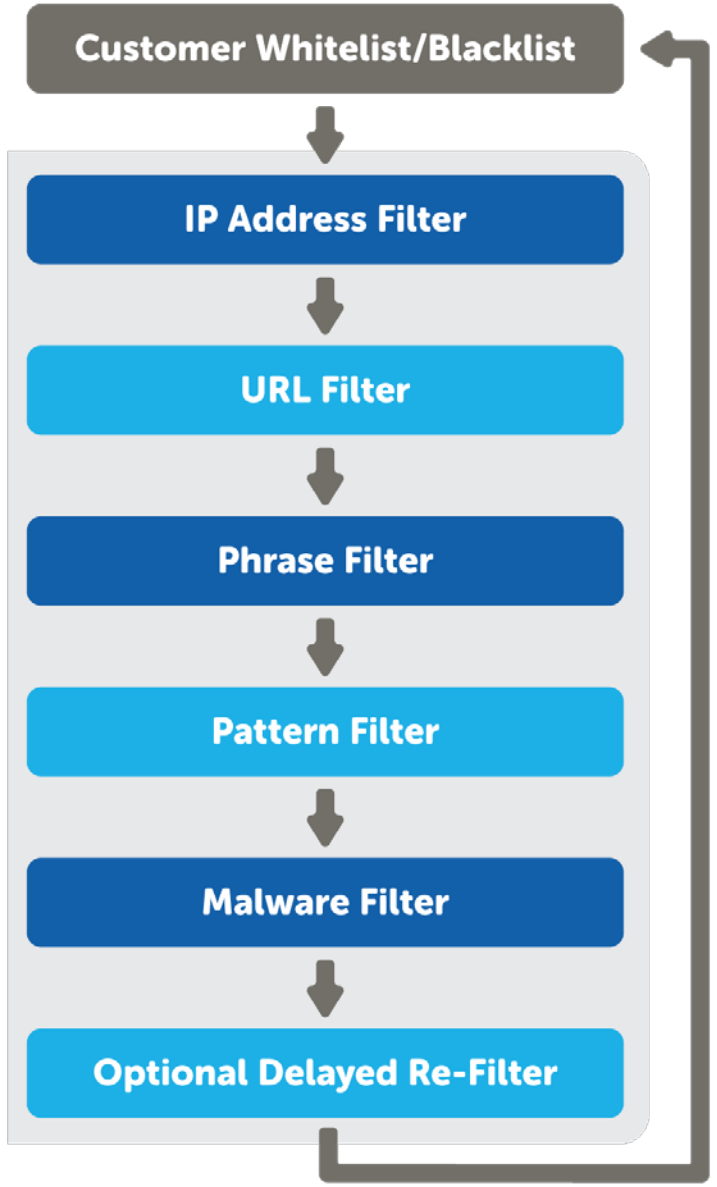
Zix provides strong protection against spam, zero-day malware, ransomware and phishing.

- Blocks 99.5% of spam and 99.99% of all malware
- Passes 99.999% of legitimate email
- Machine learning and live threat analysis provide the strongest protection
- No tuning or training required – immediate protection, minimal impact
- Outbound filtering to protect your reputation

Multi-Layer Filtering

Accurately identify email threats

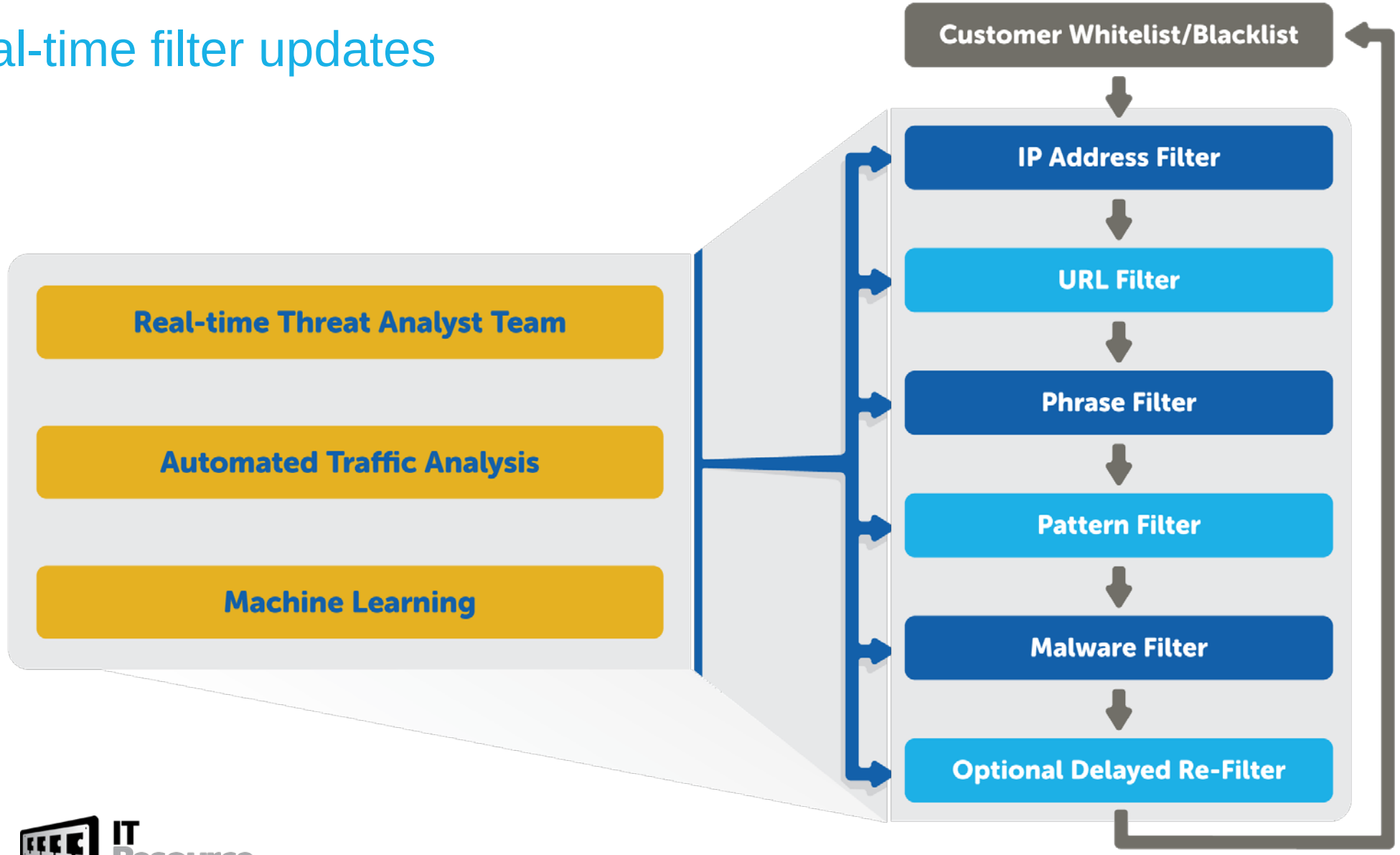
- Whitelist/Blacklist
  - Customer controlled IP blocking
- IP Address Filter
  - Block known spammers and attackers
- URL Filter
  - Protect against malicious websites
- Phrases Filter
  - Identify unique phrases only used in spam
- Pattern Filter
  - Identify complex patterns used in attacks
- Malware Filter
  - Extensive analysis file attachments
- Delayed Re-Filter
  - Re-filtering for questionable emails



zix IT Resource

Multi-Layer Filtering

Real-time filter updates



zix IT Resource

Filtering Controls

Simplicity with control

Zix threat protection is deployed with the configuration optimized for the best results but provides the controls to customize if needed.

For each level of filtering, define the action taken on unwanted emails:

- Quarantine the email for review by administrators or users
- Add warning to the email subject to notify users of potential risk
- Reject the email and notify sender or delete without notification
- Forward the email to a security officer for review

Filtering Options

Control flexibility

Customize the filters to meet your specific business needs.

- Reject emails to invalid internal recipients
- Filter emails based on the country of origin
- Create attachment filters to remove, replace or block certain file types
- Identify attachment viruses and remove from email or block email
- Enable or disable the filters for common attack methods
- And much more

Email Continuity

Protection in a disaster

Zix provides automatic disaster recovery of email with a 5-day spooling of inbound messages and 30-day email access.

If your mail system goes down, Zix provides emergency access to email:

- Inbound emails are available for up to 5 days and delivered when your mail system comes back online
- Users can send and receive emails through a web-based interface
- No disruption to Zix email encryption service
- When combined with archiving, user has access to unlimited email history

Email Encryption & Data Loss Prevention

Secure and Easy

zix®

Email Encryption Options

Sender Side

Desktop Encryption (ZixMail)

- End-to-end solution for sending and receiving encrypted email
- Ideal for protecting sensitive corporate data at rest and in transit

Gateway Encryption (ZixEncrypt)

- Policy and user controlled encryption for sensitive outbound email
- Ideal for ensuring regulatory compliance

zix IT Resource

Email DLP

Protect the primary source of data loss

Zix combines sophisticated policy rules and content scanning with an intuitive quarantine interface.

By focusing strictly on email, Zix provides a straight-forward DLP approach that:

- Addresses business's greatest source of data risk
- Decreases the complexity and cost
- Reduces deployment timelines from months to hours
- Minimizes impact on resources and workflow

Policy Controls

Control what data leaves your organization

Policy controls allow each individual email to be examined to ensure the sender and recipient are authorized to handle the information.

Define specific rules to control how each email is handled

- Control based on the sender and recipient email address or domain
- Search on message attributes such as size, file types, number of recipients and whether the message is encrypted
- Scan the subject, body and attachments for sensitive data

Based on the policy rules, decide if each email should be quarantined, blocked, branded or encrypted.

Content Filters

Prevent data loss with sophisticated filters

Pre-defined filters automatically identify and protect sensitive data, including:

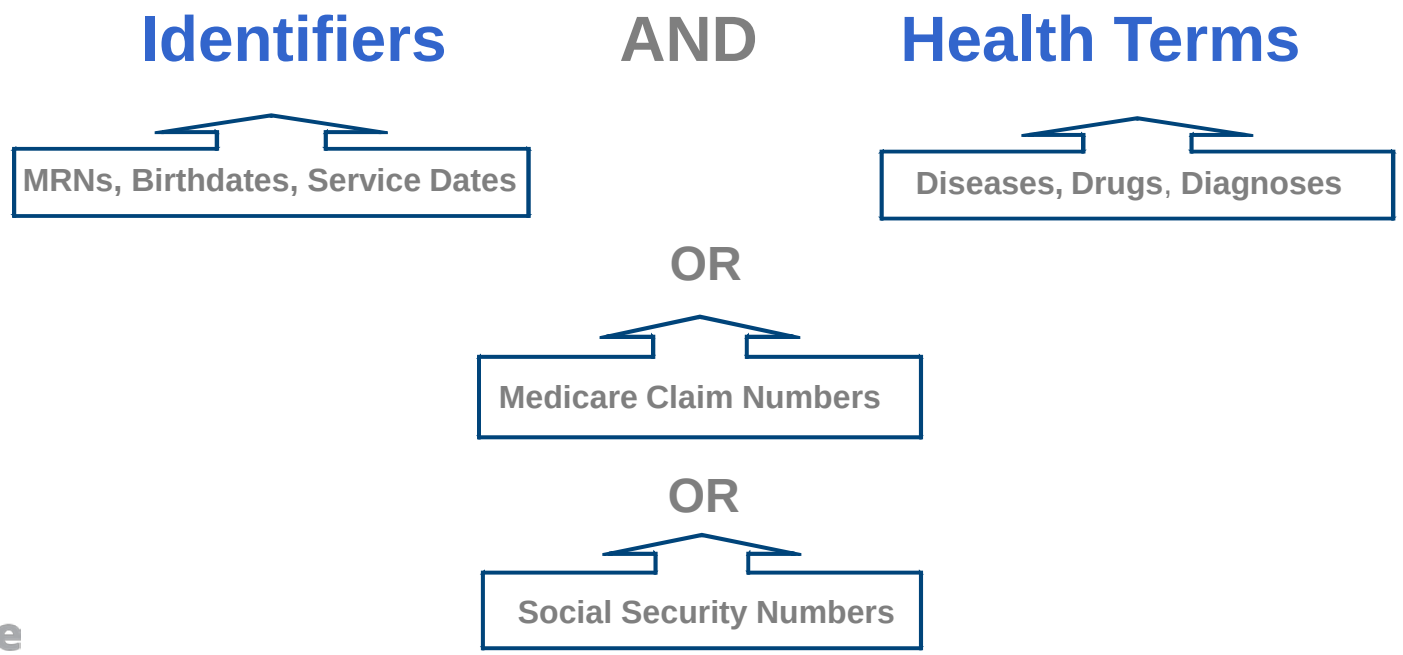
- Financial GLBA
- Healthcare HIPAA and medical research
- State privacy
- Education FERPA
- Title industry
- Human resources
- Social Security numbers
- Credit card numbers
- Profanity
- Custom filters built to your specific requirements

HIPAA Regulation Policy

Turn-key Email DLP Filters

Designed to recognize **Individually Identifiable Health Information** as defined by HIPAA Privacy Rule §160.103

Leverages a combination of filters to recognize the intersection of personal identifiers and health terms using the following logic:

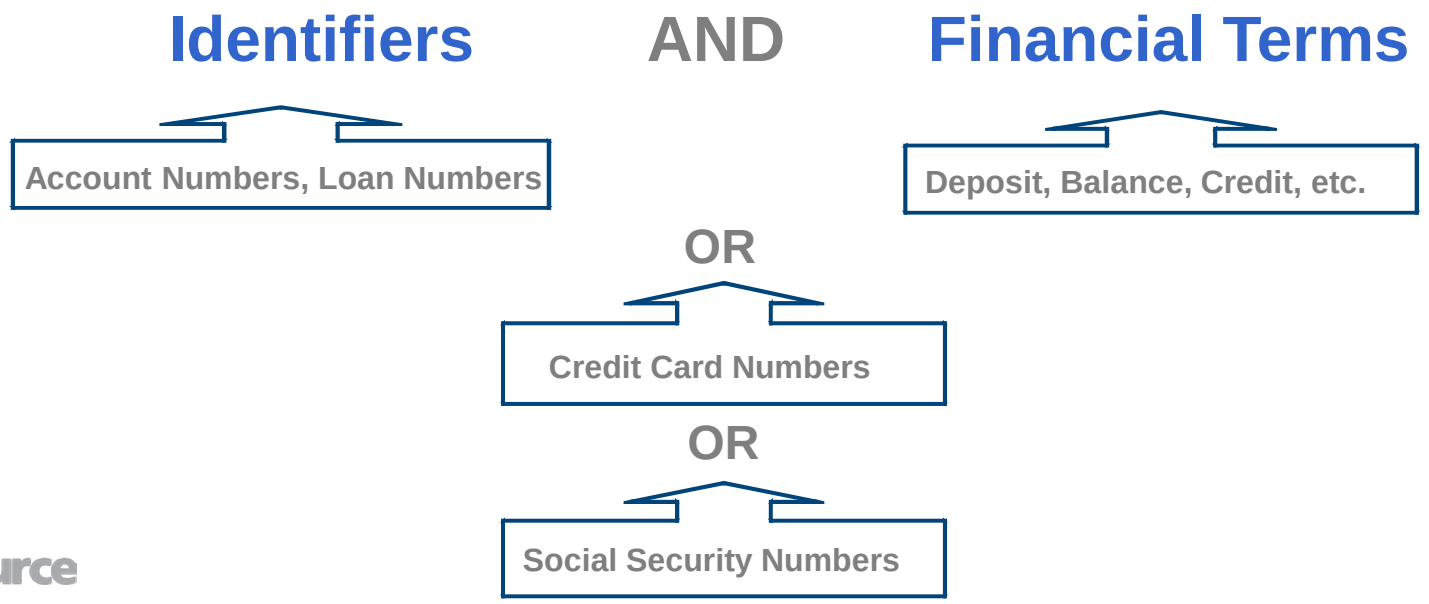


GLBA Regulation Policy

Turn-key Email DLP Filters

Designed to recognize **Personally Identifiable Financial Information** as defined by SEC, FTC, Federal Reserve and FDIC in the final *Privacy of Consumer Financial Information*.

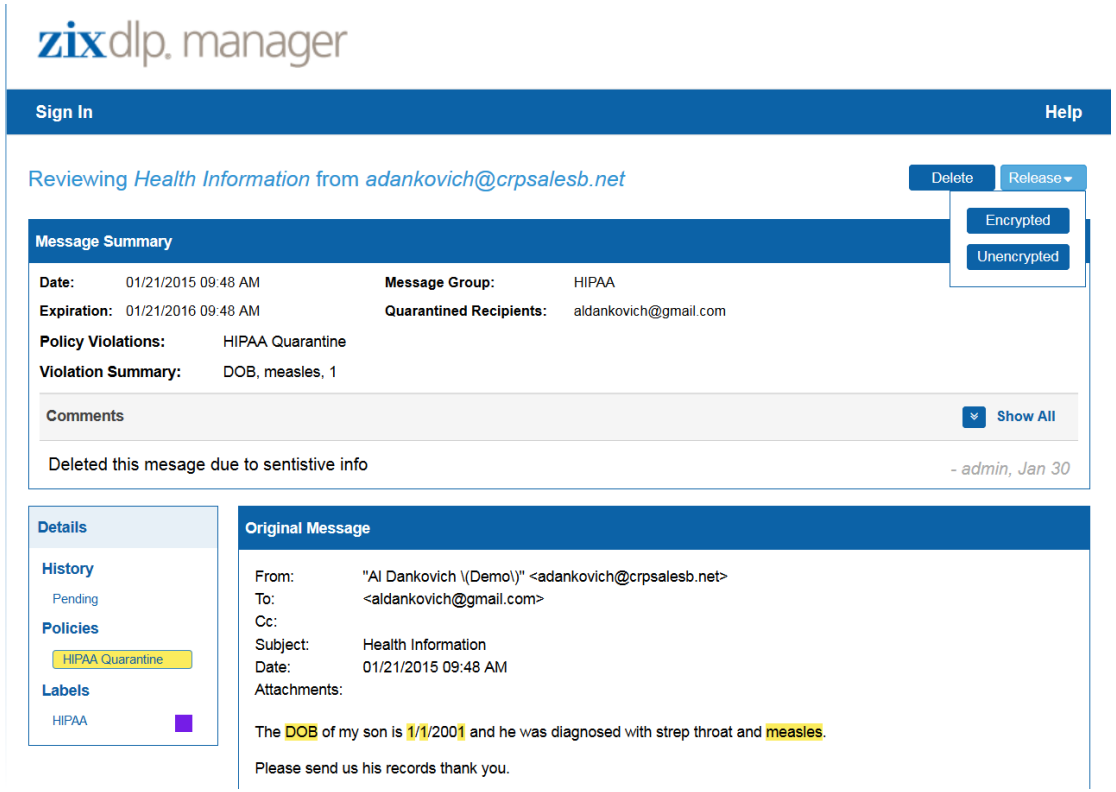
Leverages a combination of filters to recognize the intersection of financial identifiers and financial terms using the following logic:



Email Quarantine

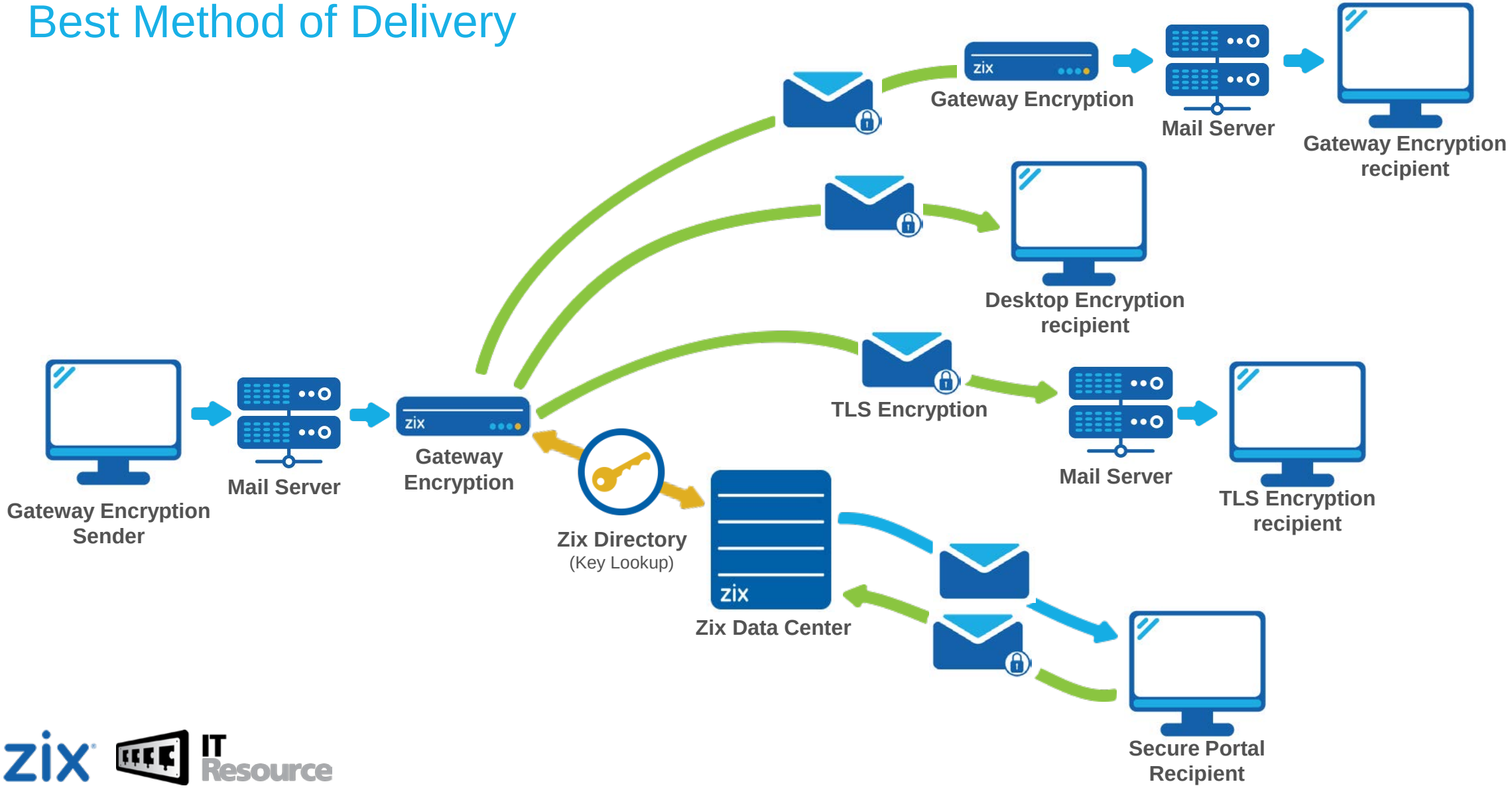
Review workflow and audit trail

- Configurable workflow allows notifying sender or compliance manager
- Train users using optional sender release with justification
- Define groups and authorized reviewers
- Automatically release emails while maintaining an audit history
- Categorize and search emails for review



Gateway Encryption

Best Method of Delivery



Gateway Encryption

Transparent encryption

Zix is the ONLY provider of fully transparent email encryption.

By removing extra steps and passwords, Zix makes secure email as easy and transparent as regular email for both senders and receivers.

Without the hassle:

- Business can continue to collaborate with ease
- Message-level encryption using S/MIME provides strong security
- Bi-directional encryption of all emails between Zix gateway encryption customers
- Compliance with regulations and company policies is no longer a burden

zix IT Resource

TLS Encryption

Zix Superior TLS

Enable Try-TLS without the risk of man-in-the-middle attacks

- Certificate authentication ensures security
- Automatic fail-over to alternate secure delivery

Policies enable control over when and how TLS is used

- Allow based on sender, recipient and message content
- Specify the level of authentication and encryption required
- Block ISPs or domains that do not provide strong security

Email is branded to alert recipient the message was sent security

This message was sent securely using Zix.

Increase the level of transparent encryption without increasing the security risk

zix IT Resource

Secure Portal Encryption

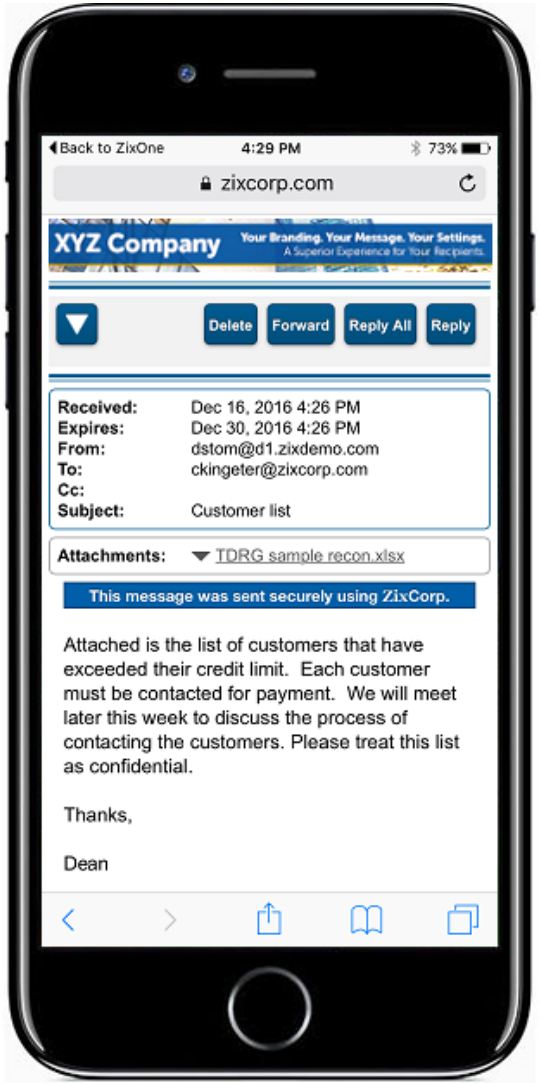
Highly customizable and easy to use

Provide your recipients with a full email experience

- Inbox, sent folder, drafts and more
- Allow users to compose secure emails
- Optimized for mobile email access

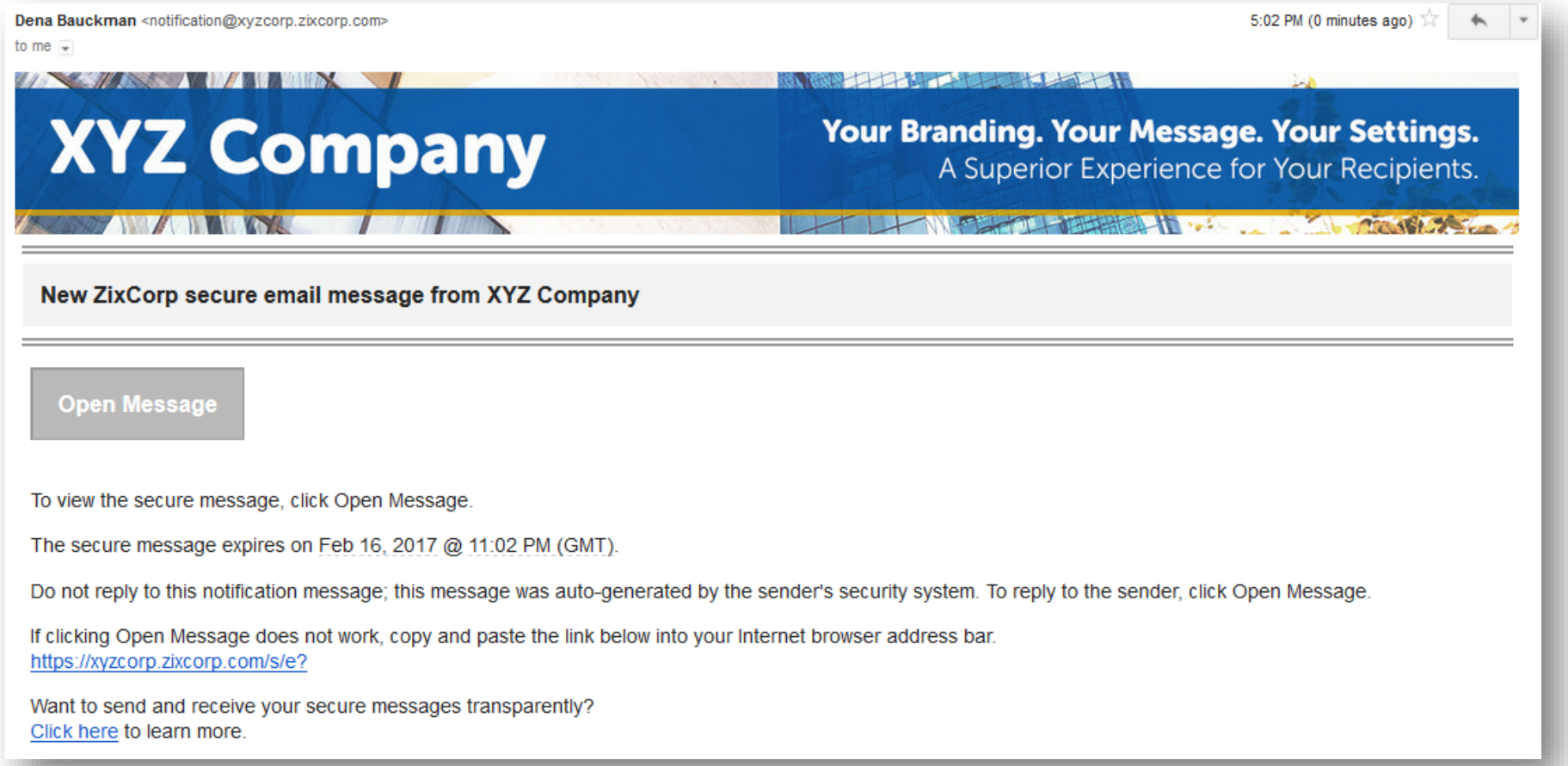
Customize the recipient experience

- Flexible branding of the portal to match your needs
- Customized the authentication, including 2-factor and Single Sign-On
- Integrate the portal into your website using iFrames
- And much more…



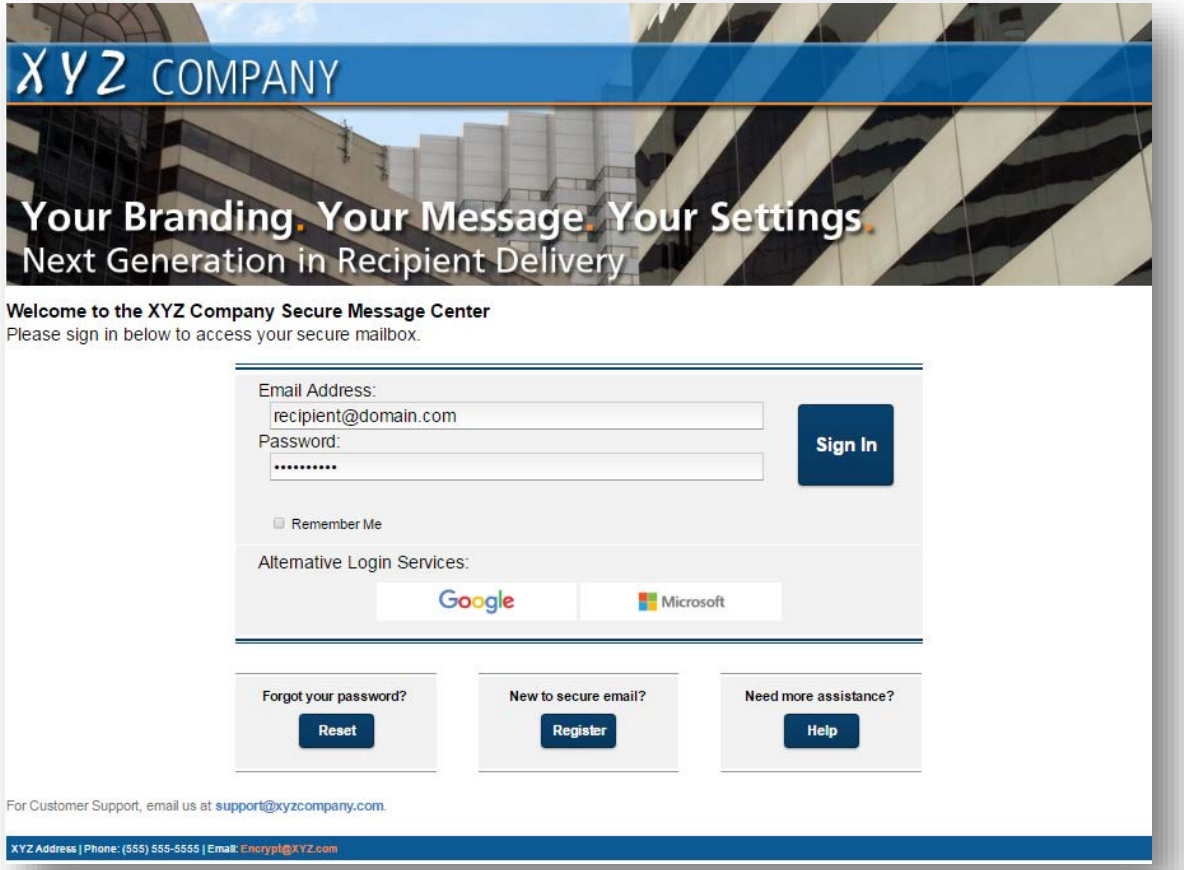
ZixPort – Desktop or Mobile

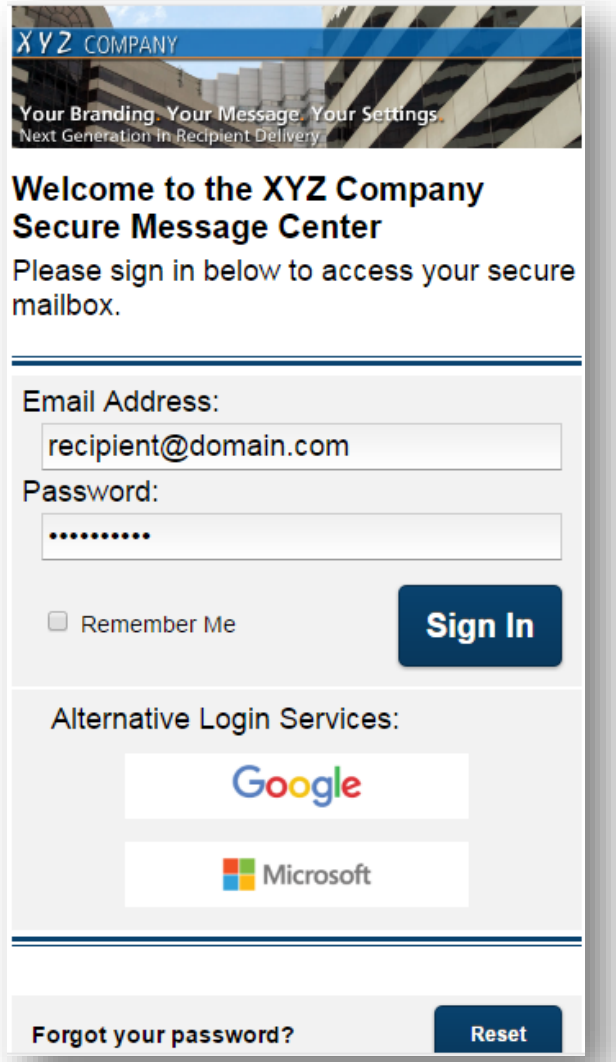
Intuitive, Flexible, and Secure



ZixPort – Desktop or Mobile

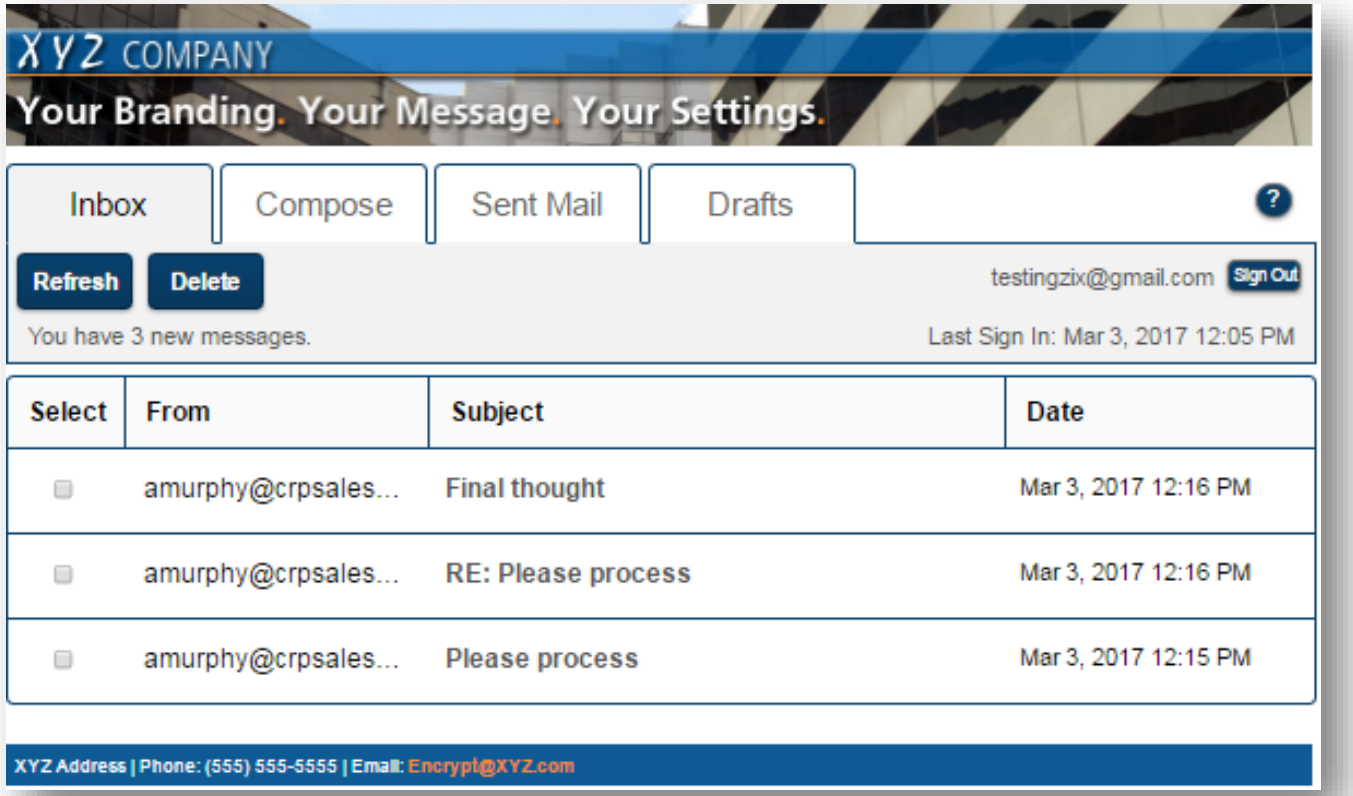
Intuitive, Flexible, and Secure

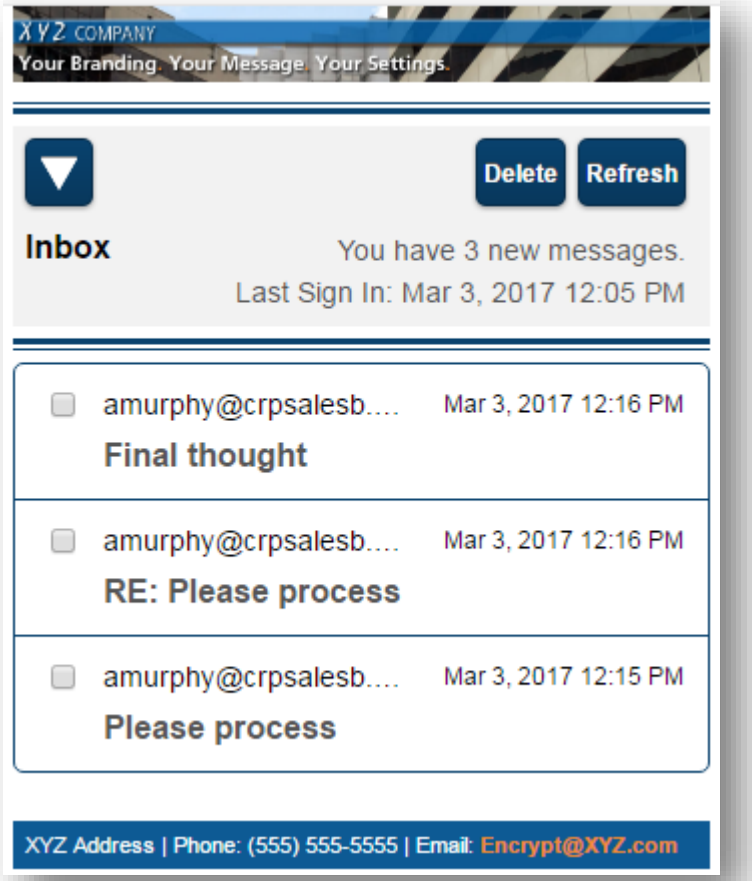




ZixPort – Desktop or Mobile

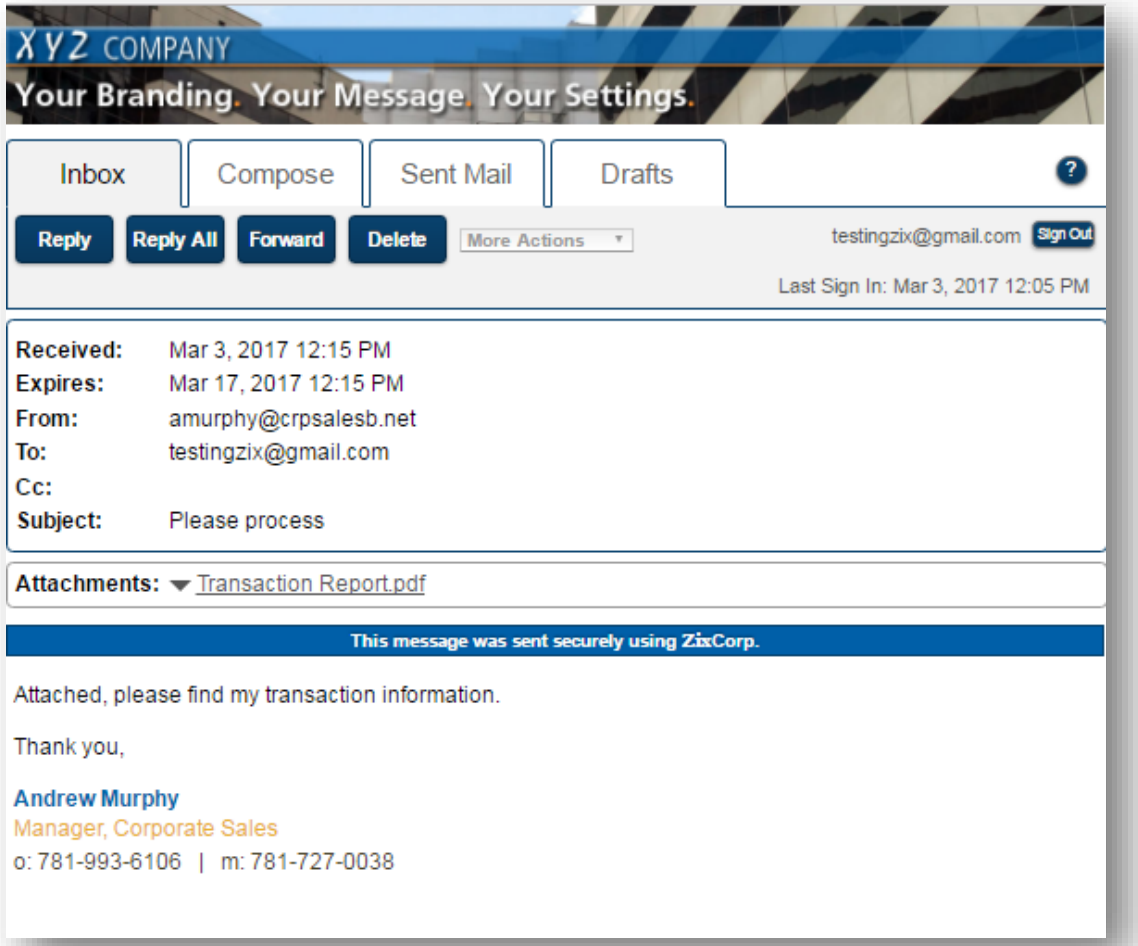
Intuitive, Flexible, and Secure

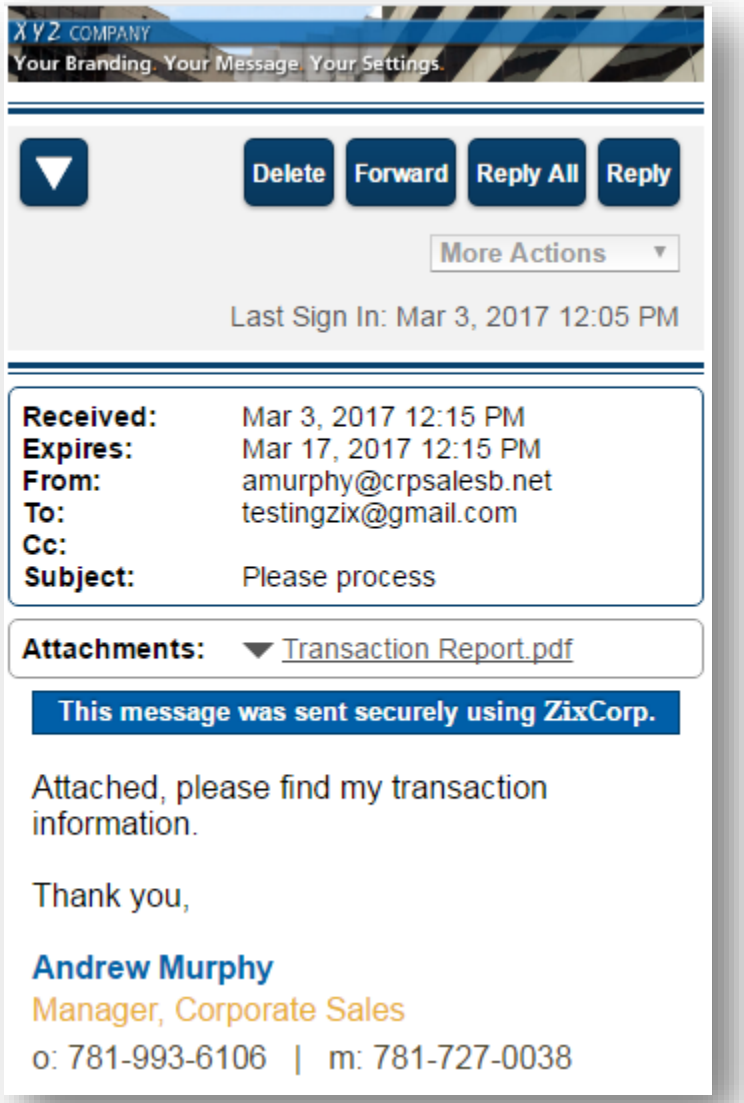




ZixPort – Desktop or Mobile

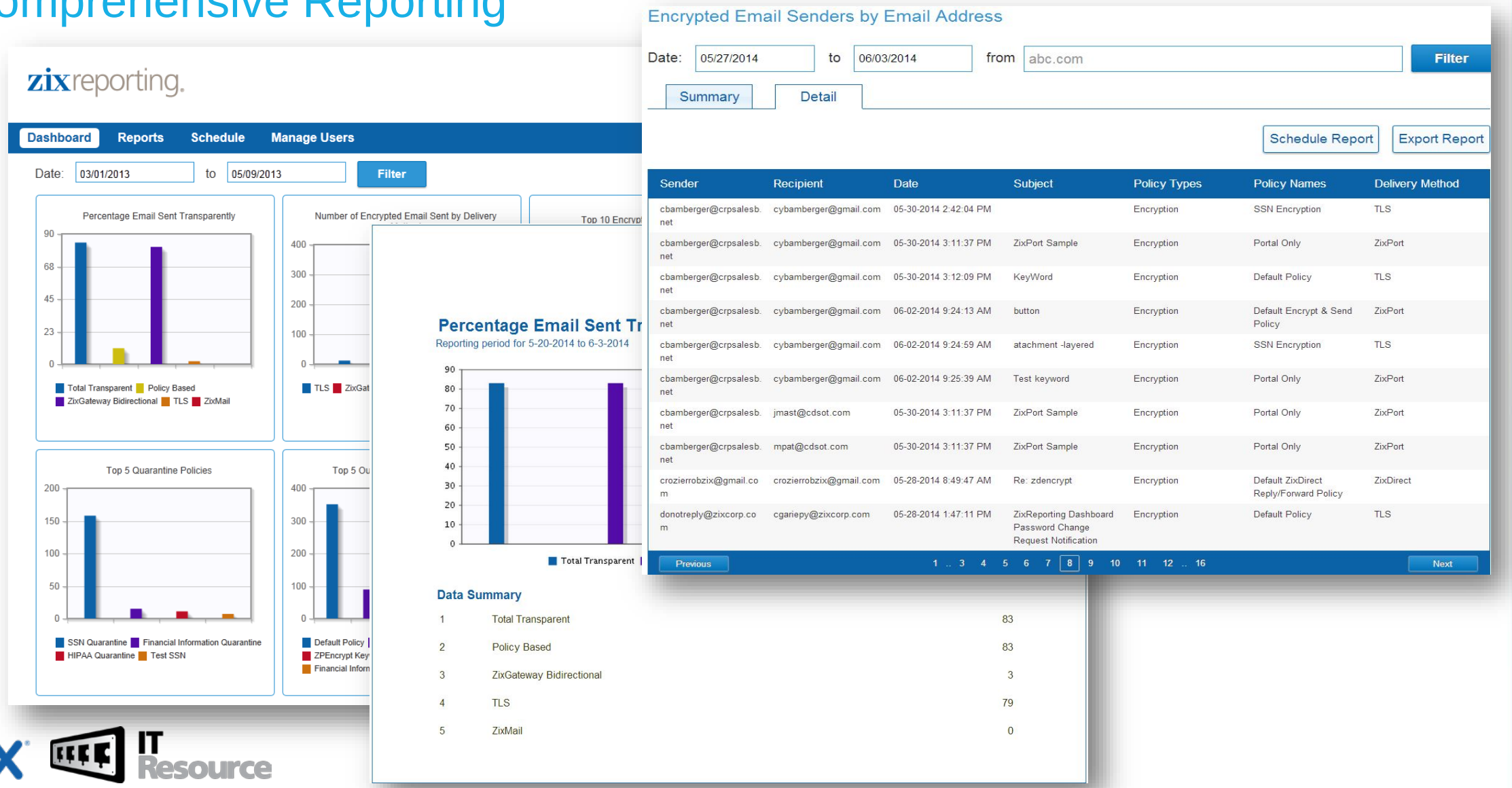
Intuitive, Flexible, and Secure





Email Encryption

Comprehensive Reporting



Your Questions & Comments

Please use the WebEx Q+A Feature to send us your questions

Thank You!

Adam Lipkowitz
Sr. Account Executive
(781) 993-6102
alipkowitz@zixcorp.com

Jenn Buchin
IT Resource
jennb@itrw.net