ZIX SECURE CLOUD—DATA LOSS PREVENTION

Protect Your Email Data Automatically with Zix Data Loss Protection

You don't have to be a compliance analyst to keep your company safe. Zix's Data Loss Prevention (DLP) filters automate email encryption, work out-of-the-box, and are highly customizable.

Current Challenges:

Exposing sensitive information is as easy as hitting "reply."

- Most companies must enforce an email data security policy (state, federal, industry)
- It's impractical for employees to always catch sensitive information
- Employees find workarounds
- Training isn't sufficient
- Blanket security policies disrupt employee productivity
- Most enterprise DLP solutions tend to be cumbersome
- Remediation workflows are slow or undefined
- Greater security concerns due to increased remote workforce
- More endpoints and increased risk of exposing sensitive data
- Less budget to execute

Solution Opportunities:

Automatically encrypt and deliver sensitive information over email

- Protection from day one—works out-of-the-box
- Industry-specific policies detect information in email subject, body, and attachments
- Best-practice approach satisfies regulators and governance
- Policy-builder to select the right combination of filters for your industry
- Free customization service to fine-tune filters
- Greater awareness—managers can review messages
- Implicit training—employees see why emails were flagged
- Identify employees in need of training

Benefit

Secure email data without sacrificing productivity.

- Get up and running quickly without being a filtering expert
- Gain visibility into sensitive information on your email network
- Access to filtering experts
- Simple DLP incident investigation and remediation
- Periodic updates for your industry

Zix DLP capabilities

Gold-standard email encryption with automatic enforcement with flexible policies:

- Automate custom notifications to explain actions to users
- Define your policy for reviewing or quarantining to/from unauthorized users
- Delegate outbound quarantine management to managers
- Manage quarantined messages with flexible searches and filtering
- Release or delete individual or multiple quarantined messages with one click
- Monitor quarantine activities and trends via reporting

Industry-leading filtering and encryption | Periodic updates | Works immediately | Customizable

Zix DLP Email Filters

Zix's filters are designed to be 99% accurate out-of-the-box. They were created with the help of regulatory experts and in partnership with our customers, who helped us tune the filters using decades of real business email messages. The filters continue to evolve and are regularly updated by our Zix Research Center, who can also create unique filters for our customers at no extra cost.

Automate your encryption

Empower users to conduct business without worrying that somewhere deep in the email thread lies sensitive information. Because, even if the user knows best, the average person sends hundreds of emails and can't check them all.

People are also working longer hours and are more prone to mistakes, typos, and errors of inclusion. On top of that, there's no guarantee that every employee is taking security seriously, despite training, and that includes contractors who may receive no training at all.

In one example, a collection department trained staff to delete account numbers from subject lines when replying to emails from a vendor. Zix's DLP filters uncovered that employees were missing account numbers hidden in the body of the message and within the email thread.

Gain insight into sensitive information within email

- **Test filters before activating automation rules.** This helps you better understand what information users or departments are handling, uncover individuals who need training, or to customize and tune new filters.
- **Improve security awareness by notifying employees when messages automatically encrypt.** If the user forgets to encrypt an email, the filter encrypts and then notifies them, highlighting the confidential words, phrases, or attachments.
- **Understand context.** Did the employee reply to a message with sensitive information already in it, or did they attach the file?
- **Prove the system's effectiveness to auditors.** Easily provide examples or identify employees in need of additional training.

Empower Users with a Quarantine

- **Give employees the final say over whether or not to encrypt an email.** For organizations that don't wish to completely automate encryption, Zix can simply hold a message for review by the sender (or a manager), highlight the content that triggered the policy, and allow the sender to release the message with or without encryption along with a typed justification for audit purposes.

  Example: In one widely publicized incident, an employee at Boeing emailed a spreadsheet to his wife, asking for formatting help. He didn't realize it contained 36,000 employee social security numbers.

- **Stop messages sent by unauthorized users and hold for review by the manager.** For example, a bank teller sending financial data externally or an intern sending customer data to a personal account.

- **Stop inappropriate content.** Block any documents that contain an "Internal Only" header or any message containing profanity.

Why change, and why now?

Email is the most commonly used communication tool in business, particularly in the era of remote work. It enables organizations to conveniently collaborate and share valuable information with external customers and partners. But people are busy and it's easy to forget that email isn't secure.

People are busy and it's easy to forget that email isn't secure

Personally identifiable information within email messages and attachments can lead to data breaches, resulting in reputational risks and high costs. According to the Ponemon Institute's Cost of a Data Breach Report for 2020, it could be $150 per record, and files could contain tens of thousands of records.

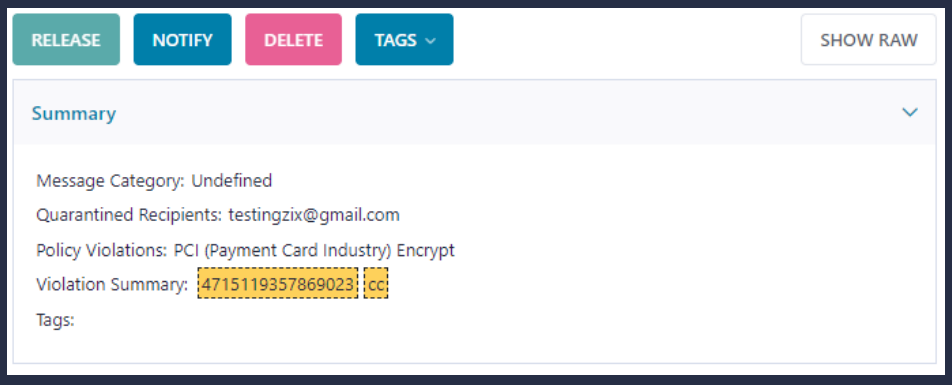
Many organizations turn to Data Loss Prevention (DLP) solutions to protect email. According to Gartner, however, most enterprise DLP solutions live up to their reputation as being difficult to implement or see value from. This can be particularly true for email because DLP solutions are often challenged with detecting the various forms that unstructured data can take within email – often creating false positives, slowing the flow of email, and potentially driving employees to bypass corporate email by turning to alternative solutions and shadow IT.

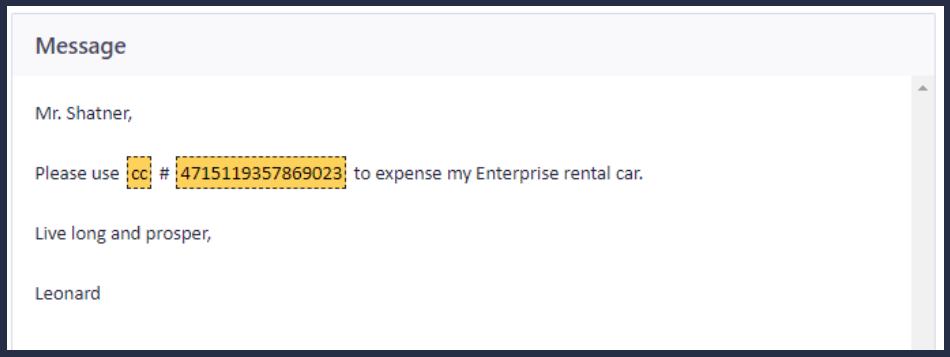
Zix's approach to email DLP is different

By focusing on what Zix does best—empowering business communication through secure email—we streamline DLP deployment, reducing the timeline from months to hours, with minimal impact on your team.

Zix DLP filters have been tuned over 20 years by real-world business email messages, ensuring they'll work for most organizations out of the box. Zix customers also benefit from a unique policy selection tool that, within minutes, guides customers to deploy nuanced filters based on their industry and specific needs.

With the Data Loss Prevention (DLP) policies built into Advanced Email Encryption, your organization can keep business running efficiently while protecting and monitoring sensitive information sent by your employees.





Example of Advanced Email Encryption's insight into what caused an email to encrypt.

It's visibility into all violations

Understanding how your employees use email and what data is leaving your organization is foundational to meeting compliance requirements and addressing encryption needs. Advanced Email Encryption provides that visibility by detecting policy violations and capturing email content without impeding communication or hindering business workflow.

Zix also helps promote awareness for your employees, letting them know when an email is encrypted due to sensitive content. The solution highlights sensitive information, helping them understand what caused the email to encrypt and where it was located.

Email messages captured through Advanced Email Encryption are easily accessible and managed. Policy violations are highlighted in the email text for quick reference. Violation summary information makes it easy to find the sensitive information located in attachments.

The deepest DLP experience in the industry

Learn more at Zix.com

zix®