Your email is one of your most valuable assets. Catch mistakes before they happen. Protect your business.

Businesses of every size, in every industry are recognizing the critical value of Secure Messaging's data leak prevention, email encryption and powerful message control.
Protecting your business against data loss is a critical step toward creating a secure communications environment. It’s also a substantial investment in time, money and resources. We know you want to get the greatest return on your IT investments. Whether you have an existing DLP solution or you are looking for one, Secure Messaging provides advanced encryption, protection and control over your data.

“Gartner Group says that 43 percent of companies were immediately put out of business by a ‘major loss’ of data, and another 51 percent permanently closed their doors within two years — leaving a mere six percent ‘survival’ rate.” (Source: Homeland Security Newswire)

**Complement and enhance your existing DLP investment**
Secure Messaging enhances your investment in DLP by delivering easy-to-use and deploy encryption and patented message control features without impacting your existing infrastructure. Route all of your email content through Secure Messaging for automatic encryption based on your policies and rules or just the content that needs encryption.

**Use Secure Messaging as a complete DLP solution**
For businesses without an existing DLP solution, Secure Messaging provides intelligent keyword scanning of all email content, including attachments and can easily be deployed to automatically encrypt content based on your security policies or industry regulations.

**Know and control what happens to every message**
Every secure message includes real-time activity notifications, so you know the moment a message has been received, read and even deleted. Users can control whether the receiver can reply to or forward a message. Messages can be instantly and fully revoked after being sent in the event of an error.
**Secure Messaging Advantages**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Email Encryption Simplified</strong></td>
<td>Secure Messaging enables users to securely send, receive, track and control email communications simply and effectively without leaving their existing email application, such as Office 365, Outlook and Gmail, and on any device including smart phones and tablets.</td>
</tr>
<tr>
<td><strong>Integration with Existing Infrastructure and Regulatory Compliance</strong></td>
<td>Secure Messaging integrates seamlessly with existing DLP engines and auto-decrypts to any archiving or journaling system to support e-discovery and other compliance requirements, such as HIPAA, FINRA, Sarbanes Oxley and other security regulations.</td>
</tr>
<tr>
<td><strong>Never Interrupts Workflow</strong></td>
<td>Secure Messaging tightly wraps around existing email infrastructure using existing email addresses and without interrupting workflow. Internal and external users can compose, send, receive and index their secure messages and file attachments directly within their usual email application on any device.</td>
</tr>
<tr>
<td><strong>Fully Customizable Encryption Environment</strong></td>
<td>Secure Messaging provides enterprises with a dedicated “slice” of the secure cloud that is fully customizable to match your security rules and policies. Customers can choose in which jurisdiction their data will be hosted. The portal is also branded and encrypted for all customers and their existing email environment to create a seamless user experience.</td>
</tr>
<tr>
<td><strong>Advanced Control</strong></td>
<td>Secure Messaging’s patented “Delivery Slip” notifies users in real-time the moment a secure email and its attachments are received and read and empowers users to control whether the message can be replied to or forwarded by recipients. Users can revoke a message after it has been sent and apply additional password protection for sensitive information.</td>
</tr>
<tr>
<td><strong>No Technical Expertise Required</strong></td>
<td>As a cloud-based solution, Secure Messaging has no hardware to install, deploys in minutes and requires no outside IT expertise to implement. Secure Messaging integrates rapidly into existing email infrastructure using existing email addresses without changing the existing infrastructure.</td>
</tr>
<tr>
<td><strong>Intelligent Keyword Scanning and Content Filtering</strong></td>
<td>Full inbound and outbound message scanning (e.g. keywords, character sequences, regular expressions, lexicons, etc.) that includes the subject line, message body and attachments to encrypt, block, or route based on policies and rules.</td>
</tr>
</tbody>
</table>
Who’s Using Secure Messaging?

Finance
Two of the top five banks in the United States have replaced their encryption tools with Secure Messaging.

Healthcare
Healthcare organizations leverage Secure Messaging’s encryption because of its seamless integration with existing infrastructure and support for HIPAA compliance.

Government
Government organizations and law firms trust Secure Messaging to ensure data is protected, secure, and can be audited and indexed for search purposes later on.
Secure Messaging: Encryption Simplified

How it works
Unlike key-based encryption which presents numerous challenges when it comes to decrypting content for regulatory compliance, archiving, searching and indexing purposes, Secure Messaging uses a non-key based platform. Messages are encrypted using the highest security standard using the most advanced cloud-based architecture.

Secure Messaging’s technology architecture allows it to easily integrate with other IT systems. This flexibility to integrate means that each secure message is not “held hostage” by a single encryption key which, for an average organization, can add up to millions of encryption keys — a nightmare for content management should these messages need to be decrypted by anyone but the receiver.

Secure messages can be received, opened, replied to, saved and indexed for search directly from within Outlook and Office 365. Secure Messaging also quickly integrates into DLP and archiving systems to allow for encrypted content to be rapidly decrypted for content scanning, storage and regulatory compliance.