

POLICY BASED ENCRYPTION SERVICE

COULD AN EMAIL CONTAINING SENSITIVE DATA PUT YOUR BUSINESS AT RISK?

ANALYST VIEW

"Content-aware security technology, which continues to grow in scope and sophistication, is proving more reliable at preventing leakage than relying on employees to follow corporate policy."

Gartner, Inc. "Understanding Data Leakage", J. Heiser, August 21 2007.

A single email containing sensitive or confidential business information could put your entire organization at risk. Data loss over email, as a result of deliberate or accidental actions, occurs everyday. Emails containing personal details, sensitive product information or confidential commercial information about business partners, could be leaving your network right now.

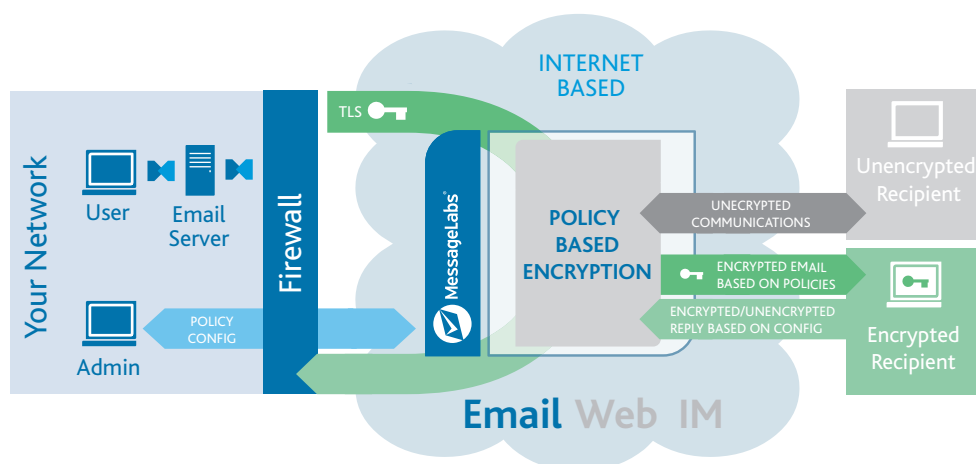
Partner relationships and corporate brand image could be badly damaged. Additionally, the real costs of investigating the breach, settling any legal issues and paying fines from industry regulators, can seriously harm your company. Due to the sheer volume of data now exchanged via email, effectively monitoring outbound emails and ensuring necessary content remains confidential can soak up huge resources.

MessageLabs Policy Based Encryption service delivers the protection you need. Enabling you to create and enforce flexible policies matching your exact requirements, the service encrypts messages - automatically, instantly, securely - based on sender/recipient information, or detailed scans of email content and attachments for words, names, phrases, numbers and file types. Recipients of encrypted mail can easily access the message, without requiring any special knowledge.

THE MESSAGELABS DIFFERENCE

- Automatic encryption with fully customizable policy rules utilizing proven content control policy engine.
- Granular scanning of all email content and attachments to identify sensitive content.
- Wide range of encrypted email delivery mechanisms, including push and pull methodologies.
- Compatibility with various platforms, including BlackBerry and Windows mobile.
- Integration with Skeptic, MessageLabs proprietary security technology for added protection against viruses and spam.
- Fully managed, easy-to-use service, no need for in-house software or appliances.
- 24/7 support and advice from dedicated MessageLabs experts.

POLICY BASED ENCRYPTION – THE MESSAGELABS WAY



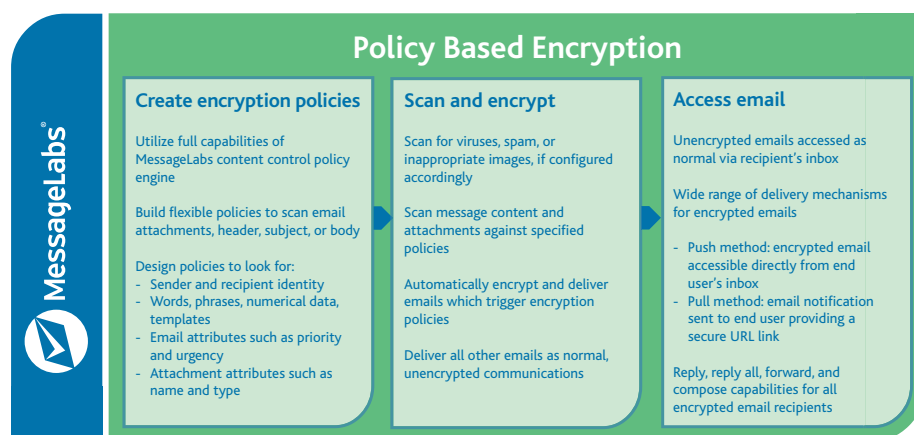
MessageLabs Policy Based Encryption service provides an easy way of controlling the main source of sensitive data loss from your company. As an added benefit, if you deploy the other MessageLabs Email Security services, all viruses, spam and inappropriate image content within your inbound and outbound emails are stopped dead in their tracks.

HOW THE SERVICE WORKS

1. You create messaging and encryption policies tailored to your specific needs.
2. Outbound emails travel between your email server and our infrastructure via a TLS (Transport Layer Security) encrypted tunnel.
3. MessageLabs scans outbound email against your policy. Email triggering a policy is encrypted automatically.
4. The recipient views encrypted email either within their inbox (push) or via a secure web portal (pull).
5. Recipients of encrypted email can send encrypted replies via a secure portal.
6. All emails benefit from Anti-virus, Anti-spam and Image Control scans (if subscribed to these MessageLabs services).

When setting up the service, you can select your preferred delivery mechanism for outbound encrypted messages. These can be sent straight to the recipient's inbox for quick and convenient access. Or the recipient can receive an email notification providing a link to a secure web portal where they can retrieve the email.

The service is fully managed and does not require installation of appliances or software by senders or recipients – regardless of whether organizations or individuals exchanging emails with your business are MessageLabs clients or have their own encryption capabilities. Nor is there any discernable delay in email delivery. Reports are simple to generate and include the number of emails that have been encrypted, originators of encrypted emails and read receipts to confirm delivery of encrypted emails.



THE MESSAGELABS EXPERIENCE

- **Email senders:** the service is easy to use, it eliminates the need for individual senders to decide what is and isn't sensitive data; no extra steps are needed to encrypt messages.
- **Email recipients:** retrieval of encrypted messages is fast and easy, while encrypted replies ensure two-way email security.
- **Service administrators:** simple set-up, configuration and report generation minimizes the burden on administrators and the end-user training needed.

NEXT STEPS

Contact a product specialist:
 APAC: +61 2 8208 7100
info@messagelabs.com

For other country offices and contact numbers, please visit:
www.messagelabs.com.au/contact

FEATURES AND BENEFITS OF THE POLICY BASED ENCRYPTION SERVICE

Features	Benefits
Automatic encryption of sensitive emails	Minimizes rogue emails leaking confidential data; facilitates regulatory compliance
Wide range of email delivery mechanisms	Provides easy access to encrypted emails
Secure reply and compose capabilities	Allows secure, two-way emailing for all recipients
Read receipts automatically forwarded to email senders	Provides confidence that messages are successfully delivered
Compatibility with various platforms, including BlackBerry and Windows mobile	Supports sender platforms; no need for contacts to have encryption capabilities
Simple to set up, configure, and use, and easy to generate reports	Minimizes burden on administrators and users; detailed reporting enables policy refinement and simplified auditing
Integration with MessageLabs proven security services, leveraging proprietary Skeptic Technology	Provides comprehensive email security and protection for encrypted mail
Fully managed service, including management of encryption keys	Reduces IT management and costs with no need for software, appliances or upgrades