

# Symantec MessageLabs Email Boundary Encryption.cloud

## Analyst View

Symantec.cloud is positioned in the “Leader” quadrant in the Magic Quadrant for Secure Email Gateways.

Gartner defines “Leaders” as vendors that are performing well today, have a clear vision of market direction and are actively seeking competencies to sustain their leadership position in the market.

## The Symantec.cloud Difference

- Total email confidentiality ensured by encryption of every part of all messages sent and received
- Cost-effective, affordable method of ensuring the integrity of email communications
- Harnesses Transport Layer Security (TLS) to encrypt the whole email connection between sender and recipient network boundaries, not just the email content
- Requires minimal on-premise management and avoids the need to use or invest in complicated on-premise hardware or software
- Operates seamlessly alongside other Symantec.cloud services, enabling all email security needs to be met with one provider

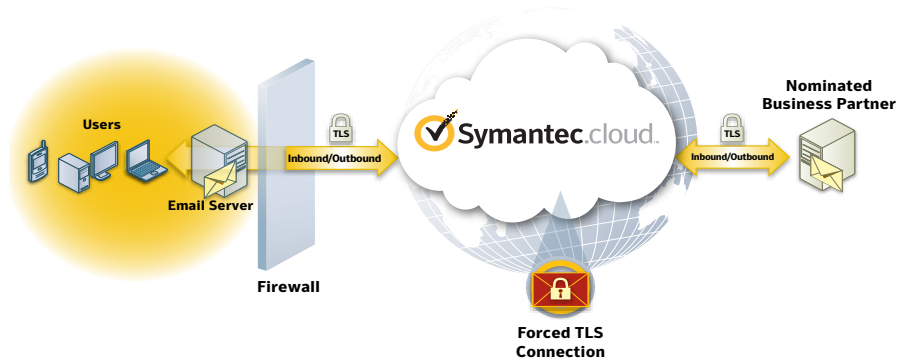
## How secure are your email communications?

Email is firmly established as a key business communication channel. However, communicating using email involves risks. Intellectual property or other sensitive information may be intercepted and then read, deleted or altered before it reaches its intended destination. Regulations and legislations are increasingly holding businesses responsible for safeguarding the confidentiality of the information they send via email.

Despite the potential consequences of failing to ensure adequate protection, many organizations do not take the steps necessary to safeguard the privacy and integrity of their email communications. Furthermore, although encrypting email generally represents the best solution, not all of the encryption services currently available offer businesses the certainty, ease-of-use and affordability they require.

Symantec MessageLabs Email Boundary Encryption.cloud service ensures the complete confidentiality of email communications and all the information they contain. It achieves this by setting up unbreachable private email networks linking our clients with their nominated partners. Every single email sent or received via these networks is fully and securely encrypted, but the application of encryption remains totally transparent to both sender and recipient.

## Secure private networks: How our solution works



Easy to enable and requiring minimal management, the Email Boundary Encryption.cloud service outperforms rival encryption offerings, not just by providing a higher level of protection but also by permitting the scanning of all encrypted email (incoming and outgoing) for viruses, spam and other inappropriate content for clients taking those specific services.

The service is based on the use of TLS to encrypt the whole email connection, or ‘pipe’, between your mail server and your partners’ or clients’ mail servers. It empowers you to define and manage a bespoke secure community for email exchange, based on a clearly defined, completely comprehensible and automatically enforced encryption policy.

### How the service works

- Symantec.cloud clients designate the mail domains they want encrypted
- Clients identify the partners they want to exchange encrypted communications
- Symantec.cloud sets up a secure private email network that uses TLS encrypted tunnels
- All emails sent between our clients' mail server and the clients' designated partners travel via this secured network
- Symantec.cloud authenticates mail server certificates, with messages only sent to authenticated servers
- We ensure the integrity of the encrypted communications and apply any additional service settings that are needed
- If a secure TLS connection cannot be established end to end, the email is not delivered and the sender is notified – there is never any 'fallback' to unencrypted delivery

### Mail Server Compatibility

- Symantec MessageLabs Email Boundary Encryption.cloud service is interoperable with all market leading mail servers, including Microsoft® Exchange, Lotus® Domino and Sendmail®
- Microsoft® is emphasizing TLS for confidentiality with Exchange 2010, reinforcing our TLS-based encryption solution
- The BITS consortium, representing 100 of the largest financial institutions in the US, advocates the use of TLS to enhance email security to protect customers and their accounts from identity theft and account fraud; and to ensure the reliability of email

### Boundary Encryption

Some confidentiality solutions only encrypt the message content, while others send messages unencrypted if a secure connection cannot be established. With the Email Boundary Encryption.cloud service, if a secure connection cannot be established, the email is not sent. Moreover, the whole of a message is encrypted (including subject line and the names of the sender, recipient and those copied in) as well as the body text and any attachments, preventing unauthorized in-transit modification.

Our solution also eliminates the need to set up, configure or maintain in-house appliances, gateway systems or plug-in software. It requires absolutely no changes in user behavior and the maintenance of only one encrypted channel with Symantec.cloud.

The net result is a service that secures email passing between sender and recipient networks, facilitates compliance with privacy and other regulations (such as the Health Insurance Portability and Accountability Act and Gramm-Leach-Bliley Act, etc.), and minimizes the overall cost that you incur.

Features	Benefits
Provides secure encryption of email communications with nominated organizations	Applies your company's encryption policies automatically and securely; facilitates your regulatory compliance measures
Fully encrypts every email sent and received within a private network	Provides easy access to encrypted emails
Automatically encrypts emails according to your specified policy	Allows secure, two-way emailing for all recipients
Encrypts email header, subject, body and attachment	Provides confidence that messages are successfully "picked up" by recipient
Encrypts email only as it passes between mail servers, the most vulnerable stage of transmission	Secure messages can be read regardless of what technology is being used by the recipient; And, there is no need for the recipients to have encryption capabilities.
Only one encrypted channel to maintain, with no additional hardware or software	Reduces IT management and costs with no need for software, appliances or upgrades
TLS authentication of mail servers, based on genuine authority-signed certificates	Ensures that encrypted email is only sent to the correct destinations

### Next Steps

Contact a product specialist:  
US: (866) 460-0000