

Symantec MessageLabs Content Control.cloud

Analyst View

Symantec.cloud, formerly MessageLabs, is positioned in the “Leader” quadrant in the Magic Quadrant for E-mail Security Boundaries.

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.

Gartner Magic Quadrant for E-mail Security Boundaries, by Arabella Hallawell, Peter Firstbrook.

The Symantec.cloud Difference

- Policy based content control service provides administrators with comprehensive, flexible and intuitive rule-building processes
- Straightforward administrator interface and set-up minimizes complexity and resource demands
- Scanning of text within multiple components of email and within supported Microsoft® Office™ and PDF attachments
- Configurable notifications on a per rule basis for all action types
- Complements Symantec.cloud services for Symantec MessageLabs Email Security.cloud, Image Control.cloud, and Policy Based Encryption.cloud

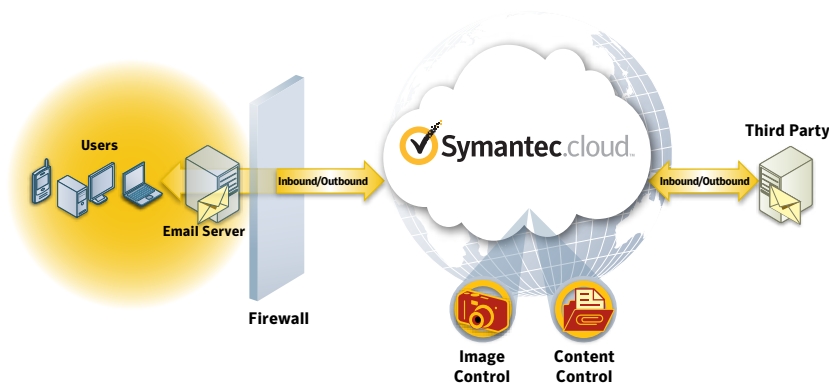
How Do You Enforce Your Email Communication Policies?

Email has become the primary communication vehicle for today’s corporations, making it essential for businesses to monitor the content of all messages entering and leaving their networks. Failure to do so can result in confidential, offensive, inappropriate or time-wasting messages compromising your email communications.

This can have serious implications in terms of damage to brand and reputation, loss of confidential data, and lost employee productivity. Moreover, failure to comply with employee protection regulations in areas such as bullying and sexual harassment, which can be perpetrated via email, may lead to legal proceedings, fines and other penalties.

The Symantec MessageLabs Email Content Control.cloud service identifies and controls confidential, malicious or inappropriate email content sent or received by your organization. Easy to set up and maintain, this cost-effective, hosted service helps to reduce the risk of data loss and enables you to establish and enforce an acceptable use policy, so employee email use can be more productive.

Email Content Control.cloud: How our solution works



Our solution harnesses a range of multi-layered technologies which determine whether or not each individual email may be allowed to enter or leave your organization. Easy to setup and maintain, an intuitive management interface provides administrators with a wealth of configuration, management and reporting functionality.

The service analyzes multiple email components including email body, subject and headers, as well as text within supported Microsoft® Office™ documents (Word, Excel, and PowerPoint versions 2000 – 2007) and PDFs that are embedded within emails or sent as attachments. Content that matches Administrator created rules is then subject to a range of actions while approved messages continue to pass through to their intended recipients.

The Gartner Magic Quadrant is copyrighted September, 2008 by Gartner, Inc., and is reused with permission. The Magic Quadrant is a graphical representation of a marketplace at and for a specific time period. It depicts Gartner's analysis of how certain vendors measure against criteria for that marketplace, as defined by Gartner. Gartner does not endorse any vendor, product or service depicted in the Magic Quadrant, and does not advise technology users to select only those vendors placed in the “Leaders” quadrant. The Magic Quadrant is intended solely as a research tool, and is not meant to be a specific guide to action. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

How the Service Works

- Inbound and outbound email is directed via Symantec.cloud, where it is scanned
- Administrators set up rules in keeping with their acceptable use policy, via the ClientNet interface
- Email which triggers a rule is subjected to a range of actions including: block/delete, redirect to administrator, copy to administrator, tag header, tag subject line, log only, and compress attachment
- Email which does not trigger a rule passes through to its intended recipient not trigger a rule passes through to its intended recipient

Service Level Agreements

Email Image Content Control is backed by a comprehensive Service Level Agreement (SLA SLA) that includes money back remedies if the following performance levels are not met:

- Delivery - 100% email delivery
- Latency – Average email scanning time within 60 seconds
- Service Availability - 100% uptime
- Technical Support - defined response times for critical,

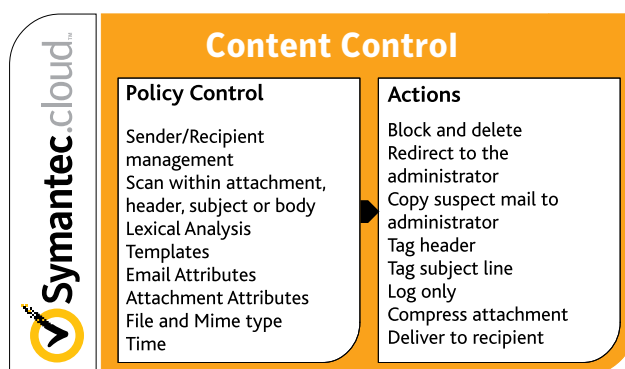
Next Steps

Contact a product specialist:
US: (866) 460-0000
info@messagelabs.com

Email messages and attachments can be scanned for keywords, phrases, URL lists or alphanumeric formulas (such as credit card, National Insurance or Social Security Numbers), all at the administrator’s discretion.

Rules can be applied to users by defining email senders or recipients as individuals, members of a group, a set of domains or a single domain. All end-user notifications for all action types can be fully configured to suit the specific rules set up by the administrator.

The Email Content Control.cloud service can be effectively combined with other Symantec.cloud services such as Symantec MessageLabs Email Security.cloud, Image Control.cloud, and Policy Based Encryption.cloud to provide comprehensive security, protection, and control for inbound and outbound email communications.



Features	Benefits
Administrator-defined policies identify and control confidential or inappropriate text-based email content	Aids enforcement of acceptable use policies, helps to meet compliance needs and reduces the risk of legal action, damage to corporate reputation and data loss
Comprehensive, flexible and intuitive rule-building processes with configurable notifications for each type of rule and action	Enables your organization’s specific email communication policies to be accommodated and notifies administrators and users of appropriate actions
Scanning within email header subject and body, as well as supported Microsoft® Office™, PDF attachments and compressed file types	Provides comprehensive protection across all email components, ensuring the appropriateness of all incoming and outgoing messages
Word list thresholds	Enables administrators to determine how often keywords or phrases must occur before a rule is triggered
Extended character list recognition of keywords or phrases in non-Western characters	Enables emails to be scanned for inappropriate content regardless of their geographical, cultural or linguistic source
Dashboard, summary, detailed and scheduled reporting	Provides visibility, accountability and confidence in the service’s effectiveness