Symantec MessageLabs Email Image Control.cloud

The Symantec.cloud Difference

- Multi-layered image control service, providing a high level of detection for offensive and inappropriate images

- Straightforward administrator interface and set-up, minimising complexity and resource demands

- Scanning of images embedded in emails and contained within supported Microsoft® Office™ and PDF attachments

- Local and global image databases, enabling administrators to optimise scanning performance

- Ability to specify individual senders and recipients who can bypass the service if required

- Complements the MessageLabs Email Content Control.cloud service, which identifies and controls confidential and inappropriate text-based email content
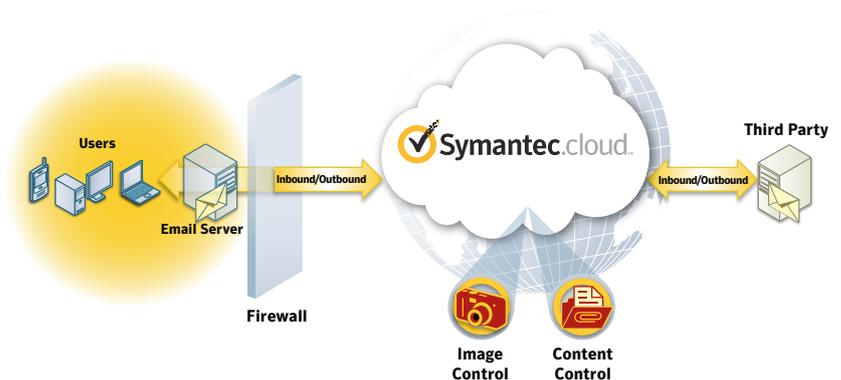
Are You Effectively Blocking Offensive And Inappropriate Images?

Email is increasingly vital for facilitating fast, effective corporate communications. As a result, it has become essential for businesses to monitor the content of messages entering and leaving their networks. Failure to do so can result in confidential, offensive, inappropriate or time-wasting messages compromising your email communications.

The circulation of images in email communications can often have serious implications in terms of damage to your reputation, productivity loss and even unapproved distribution of confidential intellectual property. 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.

MessageLabs Email Image Control.cloud service scans emails and attachments to identify, control and block inappropriate images from entering or leaving your organisation. Through the use of multi-layered filtering technologies including image composition analysis and image signatures, the service protects employees while aiding enforcement of acceptable use policies, reducing compliance and legal risks, and safeguarding corporate reputation.

Stopping Inappropriate Images: Our Comprehensive Solution

Symantec.cloud™

How The Service Works

- Inbound and outbound email is directed via Symantec.cloud, where it is scanned

- Administrators set up rules and determine sensitivity levels in keeping with their acceptable use policy

- Administrators specify which senders or recipients can bypass image scanning

- Administrators add organisation- specific images to a local approved or blocked database

- 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 and log only

- Email which does not trigger a rule passes through to its intended recipient

Service Level Agreements

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

- Email Delivery - 100% email delivery guarantee
- Latency – Average email scanning time within 60 seconds
- Service Availability - 100% uptime
- Technical Support – defined response times for critical, major and minor inquiries
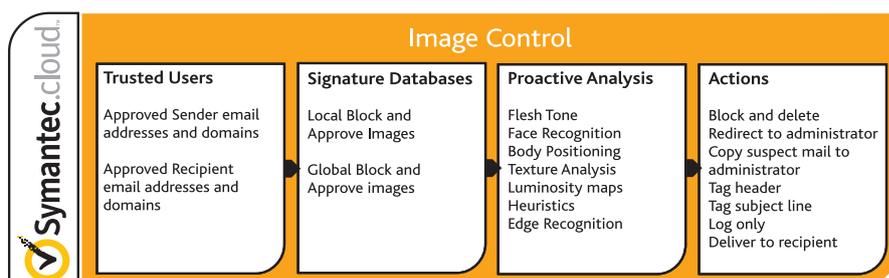
Next Steps

Contact a Xe2 product specialist:
UK: +44 (0)845 555 0000
enquiries@xe2.co.uk

The MessageLabs Email Image Control.cloud service incorporates sophisticated Image Composition Analysis (ICA) technology. Particularly well-suited to the accurate detection of pornographic images, ICA applies a comprehensive range of image-filtering algorithmic techniques, including facial recognition, body positioning analysis, texture analysis and flesh tone analysis. ICA results are fed through a sophisticated scoring system which allows the overall acceptability of an image to be determined.

A key feature of the service is enabling administrators to add permitted or blocked image signatures to a local database. This provides increased flexibility and local control over imagery, ensuring that confidential and legitimate images are accurately stopped or permitted to leave the organisation.

Approved sender and recipient lists can also be used to specify those individuals, both internal and external, that can send and/or receive emails without being scanned by the service.

Administrators can further increase the accuracy of the service by activating the additional protection of a global database of image signatures managed by Symantec.cloud containing signatures submitted by the Symantec.cloud client community.

Image Control

Trusted Users	Signature Databases	Proactive Analysis	Actions
Approved Sender email addresses and domains Approved Recipient email addresses and domains	Local Block and Approve Images Global Block and Approve images	Flesh Tone Face Recognition Body Positioning Texture Analysis Luminosity maps Heuristics Edge Recognition	Block and delete Redirect to administrator Copy suspect mail to administrator Tag header Tag subject line Log only Deliver to recipient

Features	Benefits
Multi-layered technologies designed to detect pornographic or other inappropriate image content	Protects employees, aids enforcement of acceptable use policies, reduces legal risk and safeguards corporate reputation
Configurable and highly accurate image scanning engine	Allows administrators to determine required level of sensitivity and actions to be applied
Image scanning within supported Microsoft® Office™ documents and PDFs attached to or embedded in emails	Enables administrators to activate image scanning within a range of different file formats
Customisable lists of approved senders and recipients	Permits administrators to specify internal and external users who can send or receive emails without being scanned
Customisable local image signature database	Allows administrators to maintain company-specific lists of blocked and approved image signatures
Optional global database of image signatures supplied by the Symantec.cloud global Image Community	Provides administrators with an extended database of signatures submitted by Symantec.cloud clients
Dashboard, summary, detailed and scheduled reporting	Provides visibility, accountability and confidence in the service's effectiveness

xe2 keep working at 100%