IMAGEGUARD®

Illicit Image Detection

Protection / Productivity / Profit

mailguard

> 27% of Fortune 500 companies have battled sexual harassment claims stemming from employee misuse and abuse of corporate e-mail and Internet systems.
>
> (USA Today)

IMAGEGUARD®

Illicit Image Detection

ImageGuard is a professional image filtering service that detects illicit images being distributed via both incoming and outgoing email.

The Business Challenge

Pornography continues to travel in and out of enterprise email systems, hidden within a mass of legitimate business images. This constitutes a real risk to your business in terms of legal liability, potential sexual harassment lawsuits and reputational damage.

The issue is not unsolicited pornographic spam but social communication between friends and colleagues who do not understand the possible repercussions, or do not care. As it is a social issue the only way to stamp out this behaviour is through a combination of technology, education and monitoring.

Policy Enforcement

ImageGuard is a real time pornographic image analysis and management engine that assesses all image files passing through your mail server. Using robust policy sensitivity settings, it grades image risk to determine whether or not an image may be illicit in nature.

Identify

ImageGuard provides the technology to differentiate pornographic images from the mass of legitimate business images travelling through the email gateway on a daily basis. Once the image is identified as suspect, the email filtering application is able to record other details such as sender, recipient, date and time.

Educate

Once the sender has been identified, an automatic email notification can be sent stating that the email has breached email acceptable use policy. The process educates the parties involved that this type of communication is unacceptable, and that the business has the means to identify a breach.

Monitor and Control

Email details can be logged and reported to a database for review by HR or management. These reports give the organisation clear visibility of the level of the issue and the parties involved.

A Picture Paints a Thousand Words

Never has the creation and distribution of images been easier than it is today. The growth of image capturing devices, camera phones, 3G, broadband, wireless access points and online storage now allows for an illicit image to be created, uploaded and distributed globally in seconds.

Images stored on networks and passing through corporate email systems are the legal responsibility of that company. This constitutes huge risk in terms of legal liability, potential sexual harassment lawsuits and reputation damage if email images are not monitored and filtered.

By implementing ImageGuard, combined with an Acceptable Use Policy (AUP) governing employee network access, the severe implications from misuse can be avoided.

70% of employees admit to viewing or sending adult-oriented personal e-mail at work

(NFO Worldwide)

Key Benefits

Protection from Legal Liability

There have been numerous cases in the press of high profile companies experiencing damage to their brand as a result of image mis-management . A primary risk to business is the question of legal liability and specifically, the dangers of a hostile working environment for employees.

Sexual harassment can constitute a hostile working environment if conduct is considered unwelcome, severe, and pervasive in the workplace. This may also apply if a supervisor makes sexual advances or a co-worker sends pornographic emails or shares lewd or offensive jokes, out loud, in the workplace.

In an increasingly litigious society employees are fully aware of their right to work in a safe environment. Employers now have a responsibility to provide this, and failure to do so can leave the company exposed to claims of allowing a 'Hostile working environment' to exist.

Prudent employers develop a clear Acceptable Use Policy (AUP) and deploy effective means of managing image content.

Illegal Images

The core ImageGuard engine does not specifically target or identify images of an illegal nature. However it is trained to identify pornography involving sex acts and in some instances it can offer some protection from this material.

A Duty of Care

Implementation of an image management system within a company's network demonstrates that the company has met its duty of care to its employees. In conjunction with an AUP the company can demonstrate that it employs best practice towards its employees and its infrastructure.

Protect Valuable Brand Image

A company's brand image can be damaged by employee actions, which can ultimately affect the top and bottom line, with a significant number of high profile cases involving well known companies and their employees.

By implementing a reasonable AUP and deploying image management technology companies can take precautions against such damage and its consequences.

Increased Productivity

The majority of people are suspicious of new technology and often over estimate its capabilities, resulting in a 'fear factor' being created. It has been shown that employees who are aware of image management system quickly desist from sending pornographic material and move their activities outside of the corporate network. Less time spent sharing and sending files means more time is spent on business, leading to increased productivity over time.

> 72 million visitors to pornographic websites annually, worldwide.
>
> (USA Today)

Preserve and Manage Bandwidth

Image files are, by nature, larger than text based office documents and hence consume more bandwidth and storage. By deploying image technology and dissuading employees from sending or storing inappropriate material on their network, companies can free up valuable network bandwidth.

Preserve Email Archives

Many organisations archive and store email using a service (such as SafeGuard) in order to achieve regulatory compliance. Unless filtered, any email containing an illicit image will be archived leaving a permanent record in the system.

Protect Employees from Themselves

Research has shown that it is often high profile, high salaried and important company employees who are likely to be transmitting and receiving inappropriate content. Dismissal or disciplining for network abuse can result in the potential loss of a highly valuable company asset. With an AUP and image management technology a company can take insurance against this possible loss.

Management Control of Content

In many companies network administrators will admit that they do not have any idea what potentially damaging image content is flowing in and out, and residing on their network. ImageGuard is a powerful management tool which offers companies assistance in controlling and securing their data.

> **Dow Chemical Co. fired 50 employees and disciplined 200 others after an e-mail investigation turned up hard-core pornography and violent subject matter.**
>
> (Source: Associated Press)

MailGuard.

MailGuard is one of the largest providers of SaaS managed online solutions addressing security, compliance and online management, serving thousands of clients across 18 countries.

For more information on ImageGuard or any other MailGuard service, contact:

Sales
+61 3 9694 4444 or 1300 30 44 30
sales@mailguard.com.au

Technical Support
1300 30 65 10
support@mailguard.com.au

Head Office
68-72 York Street, South Melbourne
Victoria, Australia 3205
1300 30 44 30 or +61 3 9694 4444
Fax: +61 3 9011 6110

www.mailguard.com.au

MailGuard Pty Limited