TECHNOLOGY

Overview

IRONPORT®

IronPort Image Analysis

OVERVIEW

The growth of image capturing devices along with the availability and speed of the Internet and networks has enabled users to create, upload and share illicit images globally in a matter of seconds. The problem for employers is that this abuse occurs daily on corporate networks whose contents are the legal responsibility of the directors of that company.

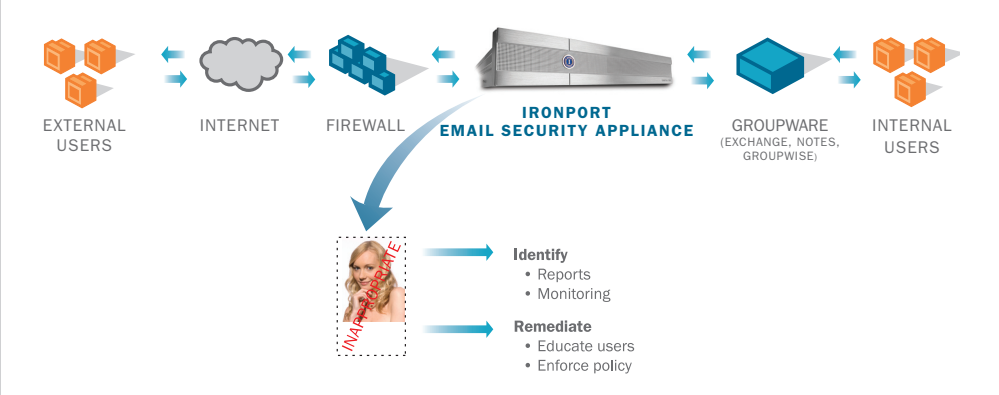
In an increasingly litigious society, employees are fully aware of their rights to work in a safe environment and employers now have a legal responsibility to provide this. In addition to legal liability issues, there are also concerns about a company's brand image being damaged by employee actions, which can ultimately affect the company's top and bottom line.

Simply put, the company is under the following risks for not tackling the issue of inappropriate content in the workplace:

- Legal liability imposed by laws and regulations
- Loss of reputation and brand image
- Decreased user productivity
- Abuse of corporate networks

In order to deal with pornography and a host of other issues companies typically implement a set of rules called Acceptable Use Policy (AUP). *IronPort Image Analysis* helps companies enforce AUP by identifying illicit images in the corporate email network. The benefits from this solution include:

- Identifying policy offenders
- Educating suspects about company policies and local laws
- Avoiding legal liability by displaying best efforts to prevent and correct harassment
- Preserving company brand image



IronPort Image Analysis uses state-of-the-art technology to detect illicit content in both incoming and outgoing email – allowing customers to identify, monitor and educate offending users.

FEATURES

Multi-layered detection is enabled during the scanning process. *IronPort Image Analysis* uses 11 different detection methods on the attachment and comes up with a verdict. Detection methods include advanced edge detection, body part separation, body part layout and more.

Configurable verdict settings are an important part of *IronPort Image Analysis*. The image analysis filter rule allows administrators to determine which actions to take, based on the following verdicts:

- **Clean:** The image is free of illicit content. The image analysis verdict is computed on the message as a whole, so a message without any images will receive a "clean" verdict if scanned.
- **Suspect:** The image may contain illicit content.
- **Inappropriate:** The image contains illicit content.

These verdicts represent a numeric value assigned by the *IronPort Image Analysis* algorithm to determine probability of illicit content. The following default values are recommended:

- **Clean:** 0 to 49
- **Suspect:** 50 to 74
- **Inappropriate:** 75 to 100

Users can fine-tune image scanning settings by configuring the values to use when determining the settings for clean, suspect, or illicit content for a particular mail profile and environment.

> 27 percent of Fortune 500 companies have battled sexual harassment claims stemming from employee misuse and abuse of corporate email and Internet systems.

— The American Management Association

Embedded image scanning allows inspection of the following types of attached and embedded files: JPEG, BMP, PNG, TIFF, GIF, TGA, ICO and PCX. When scanning image attachments, IronPort® fingerprinting determines the file type, and *IronPort Image Analysis* uses algorithms to examine the image content. If the image is embedded in another file, IronPort's content scanning engine extracts the file. The content scanning engine can extract images from more than 400 file types, including Word, Excel and PowerPoint documents.

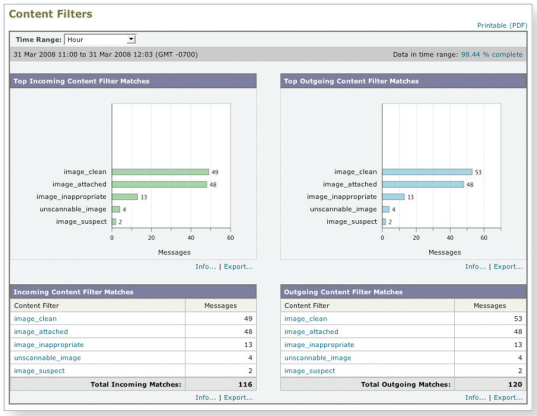
Policy integration provides the ability for users to take actions based on policy matches. *IronPort Image Analysis* integrates with message and content filters and thus enables policy-based filtering and reporting on a per-recipient or per-sender basis. The existing filtering infrastructure allows for multiple actions to be combined, based on a single filter match. For example, if the engine detects an illicit image in an email, multiple actions (like stripping the attachment, stamping with a company policy message, etc.) can be performed on it. Based on filter matches, administrators can also leverage the existing reporting functionality and create easy-to-use reports in both PDF and CSV formats. These reports can be generated 'on-demand' or scheduled for automatic generation and distribution.

> Even a successful defense against a harassment suit can cost, on average, $100,000 and the average sexual harassment verdict against an employer is more than $250,000.

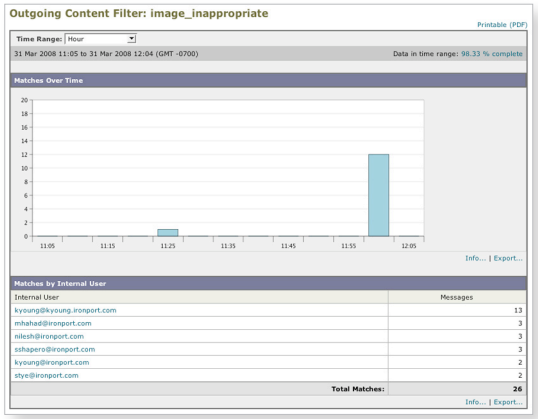
— The U.S. Equal Employment Opportunity Commission

BENEFITS

Powerful Management Many network administrators admit that they do not have any idea what inappropriate image content is flowing in and out of (or may be residing on) their network. *IronPort Image Analysis* enables a robust management tool, which allows visibility into the problem and a simple way to identify policy offenders. The easy-to-use interface and integration with content filtering and reporting infrastructure provides network administrators with a simple deployment and monitoring tool to successfully enforce company policies.



IronPort Image Analysis gives administrators visibility into inbound and outbound message content.



Quickly zero-in on users with the highest match on the policy filter.

Avoid Legal Liability In cases involving a hostile working environment, U.S. Supreme Court rulings have held employers liable for actions of employees. Various laws in places such as the Europe, Australia, New Zealand and Asia also hold employers responsible for such employee actions. Based on data collected by the U.S. Equal Employment Opportunity Commission, the average sexual harassment verdict against employers has been more than $250,000. Even in cases where employers have successfully defended themselves from such claims, the legal costs have averaged about $100,000. However, court rulings and laws have indicated that an employer may not be held legally responsible if it has taken best efforts in exercising reasonable care to prevent and promptly correct any harassing behavior. *IronPort Image Analysis* provides various detection, reporting and policy enforcement features that can help employers in defending themselves in such situations.

Preserve Brand Image Companies spend millions of dollars to develop a brand image and project that image worldwide. In financial, government and medical establishments the image is conservative, secure and professional. For large retailers, a "family friendly" image is important. The effect of negative publicity upon these carefully crafted images can be very serious – potentially leading to ridicule in the press and lost revenue. *IronPort Image Analysis* enables employers to proactively thwart such threats by monitoring corporate email messaging and taking necessary remediation steps.

Protect Employees Research has shown that it is often important and high-profile company employees who are likely to be transmitting and receiving inappropriate content. Enforcement of company policies generally results in dismissal or discipline of these employees for network abuse, resulting in loss of valuable company assets. With AUP and *IronPort Image Analysis* technology, a company can take insurance against this possible loss.

FIGURE 1.

IronPort Image Analysis is a state-of-the-art management solution that provides features to help companies enforce AUP on their email networks.

Identify
By using 11 different detection methods, the solution provides a verdict on an image.

Monitor
The solution is integrated into IronPort's existing content filtering technology — allowing users to track all incoming and outgoing email messages with illicit content.

Educate
Once abusers are identified, they can be warned about consequences. Suspects can be informed about company policies.

Enforce
The solution provides various options to enforce company policies. This includes the ability to strip questionable images or quarantine messages, copy HR or legal, notify the sender, etc.

SUMMARY

ANALYSIS AND MANAGEMENT TO ENFORCE ORGANIZATIONAL POLICIES

The distribution of pornographic and inappropriate images in and out of corporate networks represents a significant business risk to employers. Enforcement of company policies on offending users is an important step protecting organizations against the legal liabilities and brand value degradation that can arise from such offenses.

IronPort Image Analysis is an easy-to-use solution that comes integrated with the award-winning *IronPort C-Series*™ email security appliances. The solution uses state-of-the-art technology to detect illicit content in both incoming and outgoing email and allows customers to identify, monitor and educate offending users.

CONTACT US

HOW TO GET STARTED WITH IRONPORT

Through a global salesforce and reseller network, IronPort offers a "Try Before You Buy" program. IronPort has thousands of customers around the world, who realized after a short trial that this is the most advanced security technology available today. In fact, 95 percent of users that evaluate IronPort solutions become happy IronPort customers. To receive a fully-functional IronPort appliance to test in your network, free for 30 days, call 650-989-6530 or visit us on the Web at www.ironport.com/try.

TRY BEFORE YOU BUY
FREE 30-DAY TRIAL

IRONPORT IMAGE ANALYSIS
05/08
DOC RELEASE

IRONPORT®

IronPort Systems
950 Elm Avenue, San Bruno, California 94066
TEL 650.989.6500 FAX 650.989.6543
EMAIL info@ironport.com WEB www.ironport.com

IronPort Systems, now part of Cisco, is a leading provider of anti-spam, anti-virus and anti-spyware appliances for organizations ranging from small businesses to the Global 2000. IronPort appliances utilize SenderBase, the world's largest email and Web threat detection network and database. IronPort products are innovative and easy-to-use—providing breakthrough performance and playing a mission-critical role in a company's network infrastructure.

P/N 435-0240-1 5/08

IronPort is now part of Cisco.

CISCO