

Image Auditor

Effective Detection and Management of Image Risk

THE IMAGE ISSUE

It is mistakenly assumed that firewalls and anti-spam solutions will stop all illicit material entering and being distributed across the corporate network. The reality is that almost all organisations, both large and small, have illicit image content residing and being distributed over their networks. This growing issue represents a serious threat to businesses and corporate reputations.

With a growing responsibility for companies to deploy effective detection solutions, PixAlert's powerful multi-source image discovery and analysis software is a proven solution and global market leader in protecting corporate reputation, brand integrity and reducing financial risk from the distribution and storage of inappropriate content on networks.

PIXALERT'S IMAGE AUDITOR SOLUTION

Image Auditor helps organisations by rapidly scanning network resources and quickly discovering the true scope and level of risk from inappropriate images residing on their networks. It combines the most advanced image scanning technologies and best practice case management tools to deliver the ultimate in enterprise illicit image detection.

THE IMAGE AUDITOR PROCESS

- * Image Auditor runs remotely or on a local machine, and extensively scans PCs, File Servers and email accounts searching for inappropriate and illegal image files as well as movies, video clips and music files.
- * All files on selected target media are examined for image content and ranked on the basis of being inappropriate.
- * Audited images are presented to the operator in a secure management console.
- * The operator can then manage the inappropriate images through a case management interface for reporting and removal.

WHO SHOULD USE PIXALERT IMAGE AUDITOR

Image Auditor should be considered by IT Managers; IT Security Professionals; IT Audit Practitioners; Governance, Risk and Compliance Leaders and Human Resource Specialists.

Organisations who value risk visibility as a means of addressing and optimising operating efficiencies across their networks and value the integrity of their brand and corporate reputation.

PRODUCT FEATURES

* SPEED

Rapid file analysis; proven market leading throughput.

* COMPREHENSIVE

The most advanced and accurate image analysis algorithms available scanning 150 different file types including Microsoft Office documents, zip files, movies and emails (Microsoft Exchange, Microsoft Outlook, Novell GroupWise & Lotus Notes).

* AGENTLESS

No need to install software on target machines or servers.

* LOW COST DEPLOYMENT

Efficient process ensuring that audits are implemented and completed quickly.

* NON-DISRUPTIVE

Zero impact on business process.

* SCALABLE

Multi-threaded, scalable enterprise solution which ensures maximum performance across all sized organisations.

* COMPATIBLE

Compliments existing IT security, audit, governance and compliance measures.

* REVIEW & CLASSIFY

Enables management to review scan results, categorise and preview reports.

* REMOVAL

Removal of reported inappropriate content, images, videos, movies and music.

* REPORTING

Generates comprehensive reports which empower management through visible, meaningful reports with actionable features.



PRODUCT BENEFITS

* REDUCE RISK

Discover, report and eliminate inappropriate images on corporate networks

* PROTECT REPUTATION

Gain visibility required to understand the extent of the issue and act to reduce the risk of inappropriate and illegal images on networks

* GOVERNANCE

Monitor and reinforce corporate governance and internal policies

* COMPLIANCE

Measure corporate and legal compliance against client, organisational and industry standards

* AUDIT

Scan image content on network resources; desktops/laptops/file servers/emails/archive/servers

* HUMAN RESOURCES

Assists efforts in nurturing a safe, healthy and responsible working environment

* COST

Reduce potential financial risk through measurably decreasing the volume of inappropriate image material (music, film, video, etc)

* MANAGEMENT

Generate manageable and meaningful output through comprehensive management reporting features

FEATURES & SPECIFICATIONS

Image Analysis Engine

PixAlert Image Auditor uses state-of-the-art image analysis algorithms which are tuned to identify inappropriate and pornographic images. Image Auditor analyses each image using multiple image algorithms to build a statistical likelihood of inappropriateness which leads to very accurate results and reduces the false positive incidents.

Scalable Architecture

PixAlert Image Auditor has a multi threaded core built upon Microsoft's architecture, to enable it to scale to scanning across the largest enterprise networks. This ensures very high scanning performance even when scanning networks with tens of thousands of targets.

Black Lists and White Lists

WHITE LISTS: where a benign image is repeatedly displayed as a suspect image, PixAlert Image Auditor can simply add the image to the 'white list'. During future scans, these will not be returned for review and categorisation by the image analysis engines.

BLACK LISTS: PixAlert Image Auditor ships with an ever increasing database of known pornographic image signatures. Once an illicit image has been classified by an IT auditor it will be added to the black list and if encountered again the same image will automatically be added to the case file along with the description severity and categorisation applied.

PIXALERT AUDITOR SYSTEM REQUIREMENTS

PixAlert Image Auditor software is designed to run from a central management point on PCs or servers. The minimum hardware and operating system requirements detailed below refer to the auditing hardware resource, this is not a requirement for target computers whose files systems are being audited.

Minimum Hardware Requirements

- * Desktop PC or Server
- * 3 GB RAM
- * 80 GB free disk space

Operating System Requirements

- * MS Windows® XP Professional/Windows 7
- * MS Windows 2003 and 2008 Server
- * Virtual Servers

PixAlert Auditor Scans

- * Microsoft Windows® Operating Systems
- * Unix/Linux operating systems
- * Email Servers: Microsoft Exchange, Lotus Notes, Domino, Novell Groupwise
- * Email Files/Archives: PST's, NSF's
- * File Archives
- * Citrix Clients/Servers
- * Databases: Oracle, DB2, SQL Access

REPORT MODULES

PixAlert Image Auditor reporting module is capable of automatically generating many powerful management reports that enable the organisation to quickly identify and understand the greatest risk centres, thus empowering decisions through manageable and meaningful reports.

The system also has a **customised report engine** that enables clients to easily generate custom reports on the data.

PRE-PREPARED CATEGORISED REPORTS INCLUDE:

- * Top 25 offenders
- * Email distribution
- * URL source
 - Top 25 websites
- * Severity analysis

Image Owner by Severity Chart

Owner	Image Count	0	200	400	600	800
C000012	952					
C000020	704					
C000021	704					
C000011	333					
C000009	324					
C000018	226					
C000016	206					
C000013	158					
C000004	113					
C000001	108					

Legend	Count	Severity
	3335 (87.12%)	Inappropriate
	493 (12.88%)	Highly Inappropriate

Example of user severity chart from auto-generated reports