Openfind™

MailAudit Mail Audit System

Outstanding mail auditing performance with one-button regulatory compliance

The MailAudit mail audit system is a secure e-mail gateways (SEGs) solution designed for outbound data loss prevention (DLP) and e-mail encryption. Sensitive information such as contracts, business secrets or the personal information of employees and users can be blocked and the alarm rose in real-time through MailAudit's proprietary mail auditing and filtering technology. When important information is being sent out, the PKI signature encryption service of the e-mail authentication function can also be used to secure the outgoing information against unauthorized access. Users with large organizations don't need worry about blind spots in group-level policies either. MailAudit offers a hierarchical auditing framework that allows auditing conditions to be set at any level of the organization. The top-down approach provides you with the most convenient and secure mail auditing tool.

Product Benefits

Full detection of important personal and confidential information

- Flow - Prevent information from being maliciously leaked to unauthorized parties and full log archives
- Personal Information - Compound personal information auditing thresholds to prevent false-positives from signature files
- Attachments - Supports the scanning of more than 50 file formats including PDF and ZIP
- Content - Pick up illegal keywords in the mail subject or hidden within the body text

Comprehensive mail auditing process that satisfies corporate management requirements

- DLP Policy - DLP policy can be tailored to the organizational structure and individual departments
- Warning - Monitoring personnel are alerted in real-time of abnormal mail behavior
- Review - Automated or manual handling
- Reports - Visualized management of rankings and statistics for messages blocked under auditing policies

Handy helper to eliminate e-mails mis-sent due to human negligence

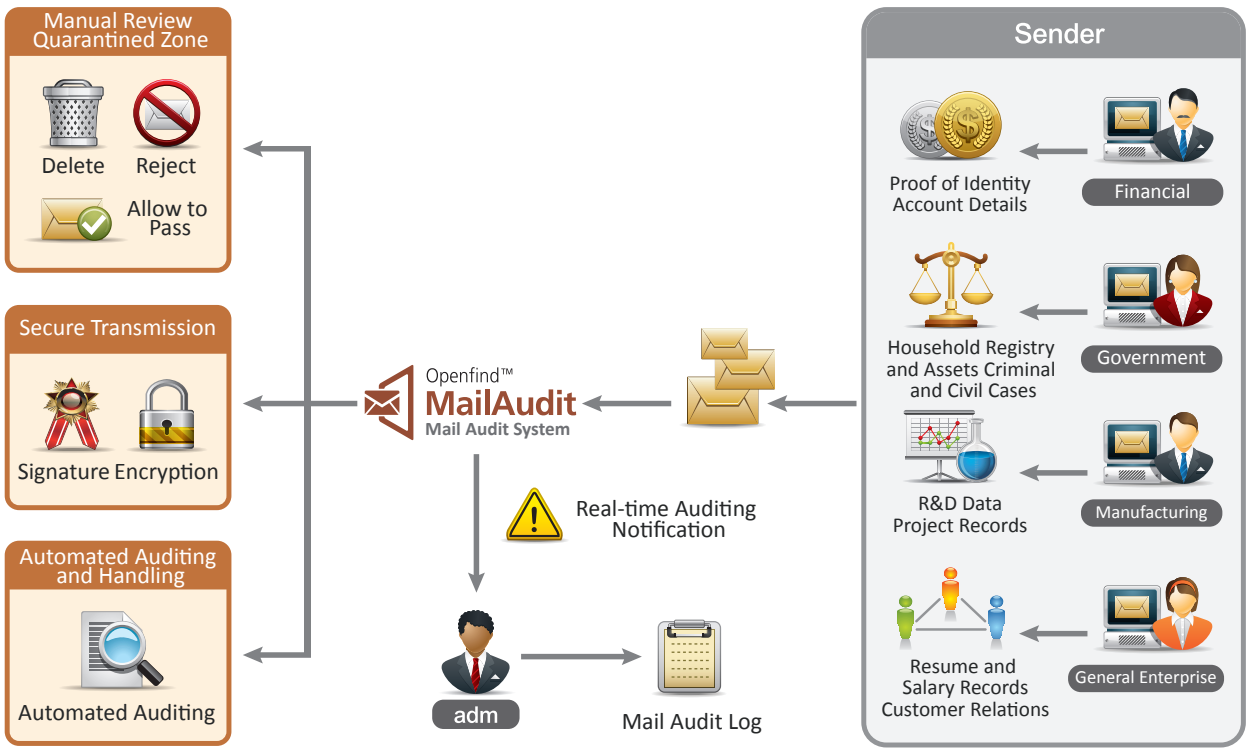
- Alert - E-mails sent to multiple people are automatically converted to blind carbon copy (BCC) to protect recipient details
- Real-time - Delayed mail delivery to allow for recovery of mis-sent e-mails
- Protection - Abnormal attempts to send large numbers of e-mails are immediately blocked to prevent system congestion
- Tracking - Convert attachments to URL for sending large files or for deleting mis-sent files

World-class bilingual information security with one-step signing and encryption

- Signature - Exclusive corporate signature that prevents the sending of counterfeit e-mails
- The PKI encryption - It used for securing important information has proven popular even with government users
- Integrated encryption with MailCloud - Mails can be set for encrypted transmission
- Exclusive PDF encryption - Background watermark to improve the confidentiality of contents and attachments

MailAudit mail audit process explained

The introduction of the Personal Information Protection Act provides for fines of over NT$200 million per case when an organization is proven to have leaked important personal information. E-mails containing all kinds of information can be thoroughly vetted using MailAudit to effectively intercept those that contain personal information such as name, birth date, contact details (e-mail, address, telephone etc.), financial information (credit card number, ID number), etc. Whenever abnormal information traffic or e-mails that may compromise sensitive information are detected, monitoring personnel are immediately notified and a full report is made available to the auditor. Normal e-mails are allowed to pass through while confidential business documents can be sent securely using corporate signatures, PKI encryption and ZIP encryption to the correct recipient.



System requirements

Recommended server-side requirements

CPU: Intel® Xeon® E3-1220 or higher
Memory: 4GB RAM or higher
Storage: 100 GB or more of disk space should be reserved when setting up a mail quarantined zone.
Operating System: Linux: RedHat Enterprise Linux 6 (64 bit), CentOS 6 (64 bit)

Recommended client-side requirements

Microsoft Edge, IE 9.0/10.0/11.0
Supports the latest version of Firefox
Supports the latest version of Chrome