

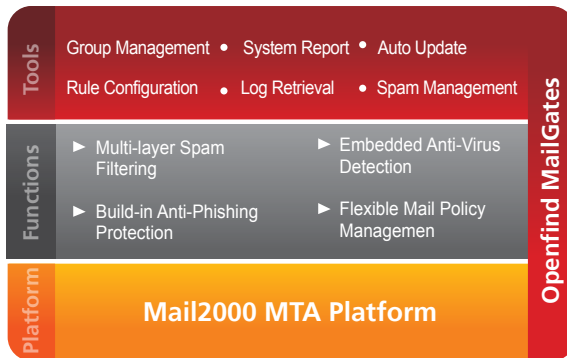
# Openfind™ MAILGATES Mail Protection System

## Product Overview

### Defense for Corporate Mail – Zero Risk for Policy Implementation

Openfind MailGates Mail Protection System is dedicated to provide a comprehensive platform for secured enterprise communication. The open structure design provides five major protection management mechanisms – System Security, Data Security, Auditing, Management, and Backup & Recovery. Inherited the excellent mail system core of Mail2000, MailGates provides highly efficient and stable SMTP dynamic network detection and protection, preventing the unsolicited mail from entering your inbox.

With the intelligent mail filter and the real-time Spam Detection Center, coupled with the functions of account integration and group management at the back-end system, MailGates can secure enterprise communication with high-quality spam detection while maintaining a very low false-positive rate.



## Product Features

### From inside to outside, the function protection, audit, and filter are all in one piece

Built in with high efficient system protection core and multi-layer spam mail filter engine and supplemented with mail audit management for a stable, clean, and safe mail environment.

### Complete and real-time graphic statistic and system reports

The complete statistical analysis reports in graphic presentation of MailGates can provide administrators with clear view of mail policy implementation and the internal mailing behaviors to ensure information confidentiality and increase business competitiveness.

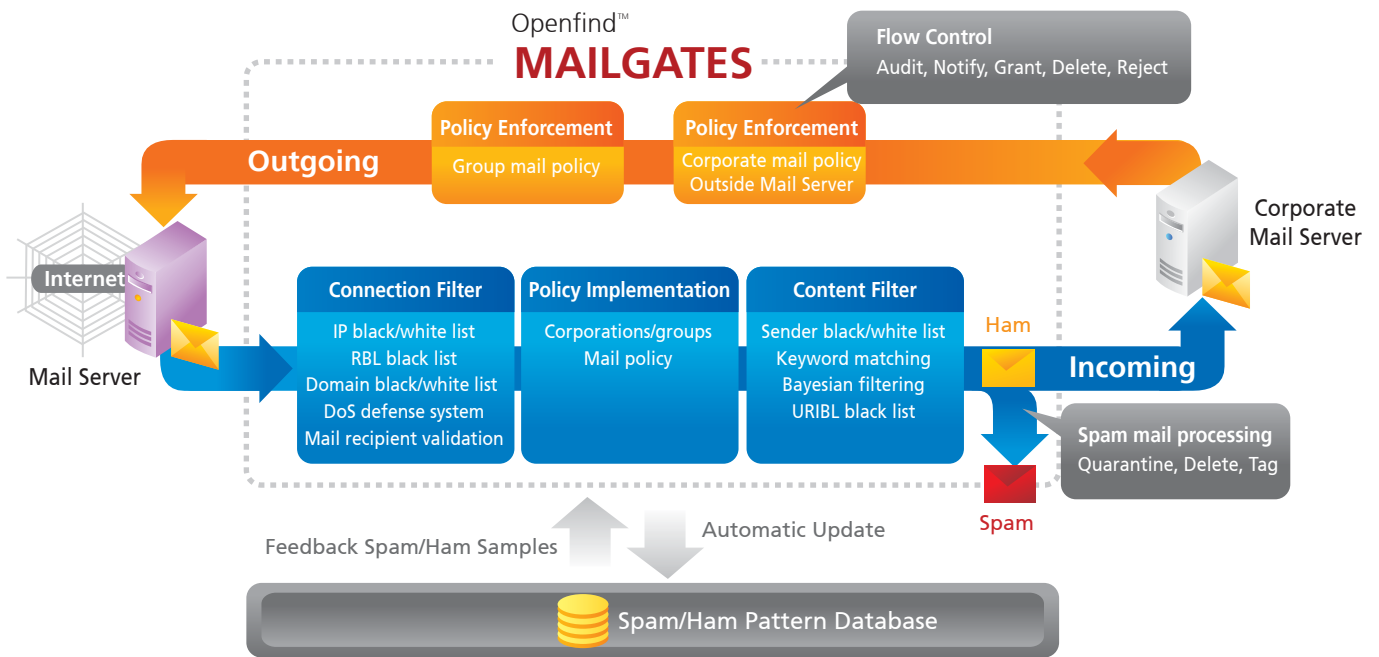


### From top to bottom, policy-based mail management for different departments

Built-in group management function allows corporations set custom-designed mail audit and filtering rules with hierarchy structures and access.

### System Requirement

Operating System	<ul style="list-style-type: none"> <li>RedHat Enterprise Linux AS/ES/WS, RedHat 9.x</li> <li>Sun Solaris 8, Sun Solaris 9</li> <li>FreeBSD 4.x, FreeBSD 5.x</li> </ul>
Browser	<ul style="list-style-type: none"> <li>Administrator: Microsoft IE 5.5 or above</li> <li>User: Microsoft IE 5.5, Firefox 1.02 or above</li> </ul>
Hardware	<ul style="list-style-type: none"> <li>CPU: Pentium 4 2.8G Hz or above (Pentium III 1G Hz minimum)</li> <li>RAM: 2GB or above (1GB minimum)</li> <li>Storage: 500MB for installation, 2GB for spam database</li> </ul>
Storage	<ul style="list-style-type: none"> <li>Estimated Disk Space: (Daily mail size) x (days to expire)</li> <li>Suggested space is " 20GB per 100 mailboxes"</li> </ul>



## Product Benefits

- Proven Carrier-Grade Technology**

With built-in optimized messaging kernel inherits high performance and scalability from Mail2000, MailGates is capable to process large-scale email transaction up to 10GB or above daily.
- Real-time SMTP Detection**

Protect from the front end of the mail server, MailGates provides DoS and DDoS defense, IP detection, and flow control. With the real-time detection, MailGates blocks abnormal SMTP connections, and save the cost on hardware and bandwidth.
- Seamless Deployment and Management**

Administrators can configure the settings through easy-to-use Web UI, consequently saves the management and maintenance efforts and greatly reduces administrative costs.
- Intelligent Multi-Layer Content Filtering**

MailGates takes advantage of various filtering methods, such as Bayesian, Black/White List, accurate with fuzzy contents filtering and keyword matching, is able to identify suspected outbreaks of spam mail through built-in large-scale data processing engine and multi-layer filtering function.
- Enhance Active Protection**

MailGates mail audit function follows corporate policy flexibly to isolate or examine the incoming and outgoing mails that match the audit criteria to ensure the security of confidential information. (i.e. sales quotes, customer lists, financial information, etc.)
- Real-time Graphic Statistics Reports**

MailGates provides comprehensive statistical reports that analyzing all filtered mail, including normal/suspicious mails, spam, viruses, audited, and SMTP connections. Administrators can easily understand the status with comprehensive statistic reports and take control the efficiency of mail policy enforcement.

For details, please visit <http://www.openfind.com>