Openfind™ MAILGATES Mail Protection System

Dual-Core Cloud Filtering for Unparalleled Anti-Spam Protection

MailGates provides a comprehensive real-time mail protection service for inbound filtering of spam, phishing, malicious and marketing e-mails. It is also the first in the industry to support IPv6 for enhanced compatibility. The collection of more than 3 billion mail samples from around the world each month along with the research and analysis of local e-mails in Taiwan allow for the comprehensive identification of spam behavior and characteristics. This in turn enables the effective detection of spam and elimination of malicious e-mails. The additional protection provided against abnormal mail behavior such as bounced mail attacks, DoS attacks and social engineering have also proven popular with users. The MailGates mail protection system is equipped with dual filtering engines that can perform localized sample analysis and global pattern recognition. It provides a dedicated solution for ensuring the security, accessibility and reliability of corporate e-mail channels.

Product Benefits

Precision filtering technology

- Global sample collection and local service analysis provides two layers of real-time anti-spam protection
- Professional URL analysis technology to effectively remove phishing e-mails and advertising URLs
- Real-time detection of abnormal connection behavior with an effective core anti-virus engine
- Exclusive automated white list mechanism for more precise mail filtering

Upgraded mail protection to ensure the security of corporate communications

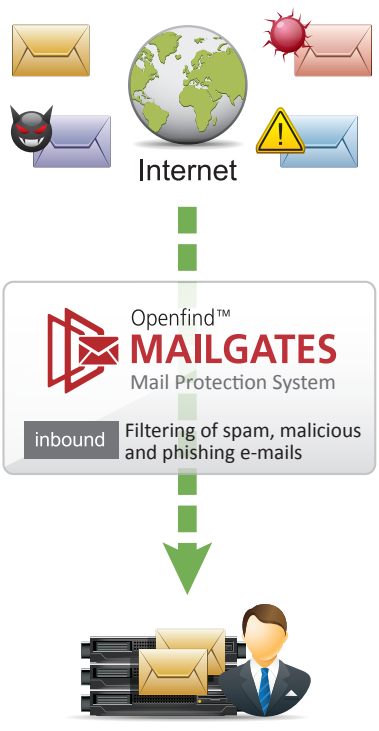
- Detect abnormal system connection frequency to effectively protect against DoS attacks
- Block massive bounced mail attacks to ensure business operations
- Active notification and removal of suspicious hyperlinks to prevent social engineering
- Protective mechanism for dictionary attacks for more accurate interception

Adjustable filtering settings and comprehensive review of corporate security requirements

- Detailed mail delivery/receiving logs for clear picture of reasons for filtering
- Protection against excessive sending of outbound e-mails to avoid becoming a springboard for spam
- Use smart gray lists and mail origin authentication to effectively block malicious e-mails
- Create tailored filtering conditions with custom IP/sender/content black/white lists

High-speed interception and report generation for optimal management efficiency

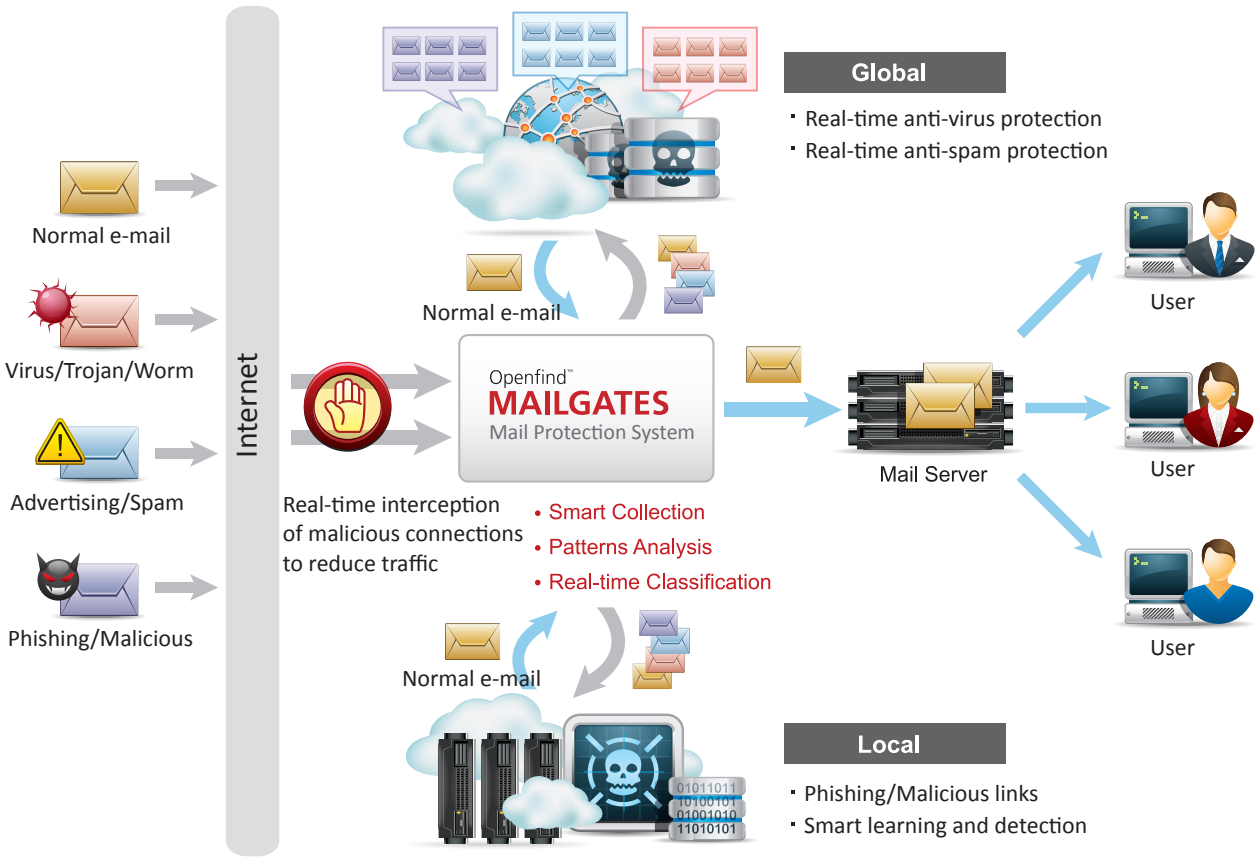
- Highly reliable telecommunications-grade mail core designed for reliable operation in big data environments
- Support for NAS and HA backups including enterprise-scale clustering architecture
- Supports graphical statistical and ranking reports with real-time protection for vulnerable accounts
- Content of intercept notifications can be customized in accordance with corporate filtering policy



Openfind MailGates mail protection system is equipped with advanced dual filtering engines that create secure channels of corporate communications

MailGates Mail Protection System

The MailGates mail protection system is deployed in front of corporate mail servers. To provide users with comprehensive anti-spam protection, global and local samples are analyzed on the mail cloud to identify all e-mail attack behaviors and threats, provide real-time anti-virus protection, as well as automatic detection and filtering of spam. The reliable and high-performance system environment, clear and succinct statistics reports and logs, as well as comprehensive and user-friendly administration functions have proven popular with users including government agencies, electronics manufacturers and educational institutions with industrial-level mail management requirements. The MailGates mail protection system will continue to refine its mail protection functions and build the most secure, smooth and reliable channel for e-mail delivery and receiving.



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