Layered Defenses and Flexible Configuration
Improve Server Performance and Security

SecurityGateway for Email Servers combines two decades of email security expertise with proven security technologies to protect message traffic from malicious attacks, message tampering and email address identity theft. Using multiple security methods, SecurityGateway assures the accurate delivery of legitimate email while minimizing the potential of false positives.

SecurityGateway incorporates multiple AV engines and proactive Outbreak Protection technology combined with additional signature recognition and heuristic analysis to detect viruses, spam, phishing, spyware and other types of unwanted and harmful email.

Data Leak Prevention rules allow administrators to easily filter messages containing sensitive information such as credit card numbers, Social Security numbers, and other types of sensitive data.

Message encryption, e-sign, and track & prove services powered by RPost provide additional privacy, collaboration, and verifiable proof of delivery, time, and exact message content.

For companies that do not have legitimate business in certain geographical locations, Location Screening allows administrators to block connections from specific countries.

Key Features

- **Accurate Threat Detection**
  Multiple analysis tools for separating threats from legitimate email
  - antispam
  - antivirus
  - antiphishing
  - antspoofing

- **Data Leak Prevention**
  An easy-to-use interface allows policies to be created which detect and prevent the unauthorized transmission of sensitive information outside of your network.

- **Expanded Security Services**
  Email encryption, e-sign, and email track & prove deliverability powered by RPost.

- **Defense Layer Customization**
  A unique control method to improve server performance. Administrators can prioritize the order in which specific security rules will execute when analyzing incoming or outgoing email traffic.

- **Comprehensive Reporting**
  Identify email traffic patterns and potential problems with comprehensive reporting. All reports support point-and-click drill-down targeting allowing further analysis to be performed.

User Control: A quarantine log email sent to users allows the release of messages or whitelisting of email without the need to burden the IT Administrator.
SecurityGateway Configuration and Features

External Threat Protection

AntiSpam
- Heuristic and Bayesian
- DNS and URI Blacklists
- Message Certification
- Greylisting
- Backscatter Protection
- Message Scoring

Antivirus
- Multiple AV engines
- Threat Signature Updates
- Recurrent Pattern Detection (RPD)
- Zero-Hour Outbreak Protection

AntiSpoofing
- Reverse Lookups
- Callback Verification

Email Authentication
- DomainKeys Identified Mail
- Sender Policy Framework (SPF)
- DMARC

Administrator Options
- Multiple Languages
- Flexible User Interface
- Domains and Users
  - Per User Options
  - Automatic Domain & User Creation
  - User Verification Source
  - Global & Domain Admin Settings
- Unlimited Account Aliases
- Per-Domain Mail Handling
- Message Quarantine Options
- Domain Level Access

Internal Threat Protection

Data Leak Prevention
Policy Enforcement via Sieve Filtering Language
Encryption: SSL & TLS
Redirect HTTP to HTTPS

RMail encryption, e-sign, and track & prove services.

Key Benefits

- Easy Administration. Intuitive, task oriented, responsive interface allows already overworked administrators to perform common actions with minimal effort. Administrative responsibilities can be delegated to a domain administrator. End users are empowered to determine the fate of a message without the need to contact the administrator.

- Proven Threat Detection. Multiple security tests, including multiple antivirus plug-ins, deliver enterprise-class protection against hidden threats, incoming and outgoing.

- On-Premise or Hosted Deployment. Per-user options for both commercial hosting and on-premise subscriptions available.

- Investment Protection. Receive free upgrades to the latest product versions for the duration of the subscription term.

System Requirements

- Microsoft Windows 10/2016/2012/7/2008/Vista/2003/XP (including 64-bit versions) (Windows server operating system recommended)
- CPU 800MHz or higher (dual core CPU 2.4GHz or higher recommended)
- 512 MB RAM (2 GB recommended)
- Network Interface Card
- TCP/IP network protocol installed
- NTFS volume with minimum of 500MB free space
- Edge 1.0, Internet Explorer 6.0, Firefox 1.5, Opera 8.5, Safari 3.0 (or later)
- Flash Player 8.0 or above for graphical reports

Internal Threat Protection

- Data Leak Prevention
- Policy Enforcement via Sieve Filtering Language
- Encryption: SSL & TLS
- Redirect HTTP to HTTPS

Performance Features

- Defense Layer Customization
- Bandwidth Throttling

Logs & Reports

- Detailed Logs
- Message Logs
- Message Log Filtering
- Historical Logs
- Real-Time Charting Reports
- Summary Report
- Inbound/Outbound Email Reports
- AntiSpam/AntiVirus Reports
- Local User Reports
- Scheduled Statistics Report

Expanded Security Services

- Message Encryption
- E-Sign
- Track & Prove Services