MailScan Secure Email Gateway (SEG)

MailScan Secure Email Gateway (SEG) is an advanced email security solution designed to protect mail servers from a wide range of email-borne threats, including viruses, spam, phishing, and malware. Positioned between the internet and the organization's mail server, MailScan SEG acts as a robust security gateway, scanning and filtering both inbound and outbound email traffic in real time.

It offers comprehensive protection through multi-layered content filtering, attachment control, anti-virus and anti-spam mechanisms, along with integrated encryption support, directory-based authentication, and detailed logging and reporting tools. MailScan SEG supports a broad range of mail servers and scales efficiently for both enterprise and SMB environments.

MailScan SEG can be deployed between the internet and the mail server in various environments, including cloud-based email platforms such as Google Workspace (Gmail) and Microsoft 365 (Office 365), as well as on-premises mail servers like Microsoft Exchange, Lotus Notes, CommuniGate Pro, VPOP3, Merak, Mailtraq, and any standard SMTP-based email system.

MailScan
Secure Email Gateway (SEG)

How It Works?

MailScan Secure Email Gateway (SEG) delivers advanced, real-time protection for cloud platforms such as Google Workspace (Gmail) and Microsoft 365 (Office 365), as well as on-premises mail servers like Microsoft Exchange, Lotus Notes, CommuniGate Pro, VPOP3, Merak, and Mailtraq. By positioning itself between the mail server and the Internet, MailScan SEG acts as a centralized checkpoint that scans and filters all email communication inbound and outbound in real time.

This architecture enhances organizational email security by enabling administrators to enforce granular mail flow policies, apply advanced content filtering rules, and maintain full visibility over email communication all without affecting system performance or user experience. MailScan SEG helps safeguard communications against spam, phishing, malware, and unauthorized data leakage while ensuring compliance with internal policies and industry regulations.

All incoming emails are routed through the SEG for inspection before being delivered to user inboxes, and outbound messages are similarly scanned before leaving the organization. This allows threats to be neutralized early and helps prevent your domain from being blacklisted due to accidental spam or malware distribution.

Beyond advanced filtering, the solution provides centralized policy management, user access control, authentication integration, and detailed logging for auditing and monitoring. Administrators can define custom rules, manage quarantined messages, and generate actionable reports to ensure secure, efficient, and compliant email communication across the organization.

Key Features

Email Security & Threat protection

Content/Spam Control

This feature enables intelligent and policy-based filtering of email messages using predefined and custom keywords or phrases present in the subject or body of emails. Administrators can create and enforce content policies to detect and prevent the transmission of sensitive, confidential, or inappropriate content, ensuring compliance and data protection.

- **Email Threat Protection**

MailScan SEG employs a multi-layered threat detection framework designed to block unsolicited, malicious, and phishing emails before they reach the user's mailbox. It leverages heuristic and behavioral analysis, real-time RBL (Real-time Blackhole List) integration, and Bayesian filtering enhanced with live threat intelligence feeds, ensuring high accuracy with minimal false positives.

- **Real-Time Email Filtering**

A policy-driven email control framework that improves both email security and visibility through multiple mechanisms. It quarantines suspicious messages for administrative review, tags potentially harmful emails with spam or virus identifiers, enforces dynamic rules based on content and sender reputation, and blocks communication from high-risk IPs, including those listed on Dynamic User Lists (DUL).

MailScan
Secure Email Gateway (SEG)

MailScan™

Key Features

Advanced Threat Scanning

Provides granular administrative control over email security by enabling inclusion or exclusion rules for specific addresses in virus scanning. It performs deep content and attachment inspection to identify concealed or polymorphic threats, and features an outbreak alert mechanism that proactively notifies administrators of emerging phishing or malware campaigns within the network.

Email Security Administration

This module provides a centralized administrative interface for configuring and controlling all email scanning and security operations related to attachments. Administrators can define how attachments are processed, scanned, and quarantined based on detected threat levels, ensuring that potential risks are mitigated before user access.

Auto-generated Spam Whitelist

The Auto-Generated Spam Whitelist automatically maintains a list of trusted email addresses excluded from spam filtering. Whenever a local user sends an email to a new recipient, MailScan automatically adds that address to the whitelist, ensuring future messages from that contact are delivered directly without being marked as spam.

Mail Disclaimer Enforcement

Customized disclaimers in MailScan SEG are automatically appended messages applied to processed emails to ensure legal compliance, confidentiality, and branding consistency. These disclaimers can be predefined or personalized and are applied to both inbound and outbound emails, ensuring that recipients always receive important organizational or legal notices.

Email Routing Configurations

Email Gateway Policy Management

MailScan SEG allows flexible configuration of both inbound and outbound email traffic, with host-level and domain-level controls. It supports direction-based mail policies and granular user/group restrictions, enabling administrators to block external communications or limit email flow between internal departments to ensure compliance and security.

Mail User Restrictions

Mail User Restrictions are an essential feature for controlling and securing organizational email communication. Administrators can define policies to allow or block emails based on sender, recipient, or domain, as well as enforce limits on message size, attachment type, and delivery scope. By restricting communication paths and filtering unwanted or malicious content, these controls strengthen system security, reduce spam traffic, and maintain overall mail server performance.

MailScan
Secure Email Gateway (SEG)

MailScan™

Key Features

SMTP Server Configuration

SMTP Server Settings (in MailScan SEG)

This feature defines the core rules governing inbound and outbound email communication. Administrators can configure routing paths, authentication methods, relay restrictions, and connection handling parameters. By combining relay control, rate limiting, and encryption policies, MailScan SEG ensures secure, efficient, and policy-compliant mail flow, protecting the organization's mail infrastructure against misuse, relay abuse, and delivery errors.

Mail Relay Configuration (ETRN)

The Extended Turn (ETRN) protocol enables secure transfer of queued or delayed emails between mail servers when the destination server is temporarily unavailable. In MailScan SEG, administrators can configure relay intervals, retry durations, and delivery rules to control when and how queued messages are retried, ensuring reliable message delivery and minimized mail queue congestion.

System Integration Support

Integration with email cloud services (E.g.: Google Workspace, Office 365, etc)

MailScan SEG integrates seamlessly with Microsoft 365 (Office 365) to deliver enhanced mail security and visibility. By routing inbound and outbound emails through an on-premises MailScan SEG gateway, organizations can apply advanced scanning, quarantine policies, and compliance enforcement before mail reaches the Microsoft cloud. This configuration ensures unified policy enforcement, auditability, and secure mail flow, preventing data leaks and unauthorized access.

Outbound Email Security (DKIM/DMARC)

MailScan SEG fully supports DKIM (DomainKeys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting & Conformance) standards to protect against spoofing, phishing, and email identity forgery. DKIM enables organizations to digitally sign outgoing messages, verifying authenticity at the recipient's end, while DMARC adds reporting and policy enforcement to block fraudulent messages. Together, they provide end-to-end trust and integrity for all outbound communication.

Greylisting

The Greylisting mechanism temporarily rejects emails from unknown or first-time senders to filter out spam. Legitimate mail servers automatically retry delivery, at which point the email is accepted, whereas most spamming systems fail to resend, effectively reducing unsolicited email traffic and enhancing overall inbox hygiene.

On-Premise Integration

MailScan SEG integrates with a wide range of on-premises mail servers, including Microsoft Exchange, Lotus Notes, VPOP3, Merak, CommuniGate Pro, and Mailtraq. It functions as a security layer between the internal mail server and the internet, scanning, filtering, and logging all incoming and outgoing messages. This ensures consistent security enforcement, compliance alignment, and seamless interoperability within mixed or hybrid environments without requiring major infrastructure changes.

MailScan
Secure Email Gateway (SEG)

MailScan™

Other Highlights

- Supports Multi-Domain and Multi-Tenant Environments
- Enables LDAP and POP3-based authenticated web administration
- Blocks image-based and obfuscated spam
- Supports automatic compression/decompression of attachments
- Allows configurable user mailbox size and quota limits
- Provides Mail Parking options for message retention and deferred delivery
- Offers comprehensive control of MailScan SEG operations via centralized console
- Includes 24×7 Free Online Technical Support and Updates

eScan®

Enterprise Security

An ISO 27001 Certified Company **Toll Free No.: 1800 267 2900** **www.escanav.com**

MicroWorld Software Services Pvt. Ltd.
CIN No.: U72200MH2000PTC127055
Tel.: +91 22 6772 2900
Email: sales@escanav.com

Awards

Partnerships

Comprehensive Protection for
SOHO • BUSINESS • CORPORATE • ENTERPRISE