

Axway MailGate

Protect your email network inside and out



As the volume of email flowing into your enterprise network increases, so does the threat of unsolicited and potentially malicious intrusions. At the same time, as your employees rely more heavily on email for official business communications and data exchange, the risk of proprietary files, intellectual property, and sensitive information leaking out also grows.

Axway MailGate™ stands guard at the Internet gateway, preventing potentially damaging messages and attachments from entering your network, and ensuring that sensitive information doesn't exit accidentally or unsecured. Combining network protection, policy-based content filtering, and automated encryption in a single, integrated solution, MailGate protects your email network inside and out, reducing administrative headaches, infrastructure costs, and the liabilities associated with unsecured and unmanaged communications.

Key Features & Benefits

Inbound threat protection

Reduce network congestion and enhance employee productivity with virus protection, anti-spam filtering, and defense against dark traffic

- Detect and eliminate viruses and other forms of malware/crimware before they can wreak havoc on your network
- Block more than 99% of unwanted email (spam) that saps employee productivity, strains network and IT resources, and creates potential legal liabilities
- Fend off distributed botnet attacks with Intelligent Edge Defense capabilities that kill up to 90% of dark email traffic at the gateway

Outbound and inbound message security and data loss prevention (DLP)

Universally enforce policies that protect confidential information and intellectual property, and ensure compliance with government regulations and corporate policies

- Prevent data loss and leakage with automated content filtering, policy enforcement, and gateway-to-gateway encryption
- Define and enforce policies based on content, users, recipients, and attachments that automatically trigger protective actions (including blocking, re-routing, and automatically encrypting messages) when a violation occurs
- Convert MS Office attachments into password-protected, locked, and watermarked PDF files to preserve document integrity
- Decrypt and inspect for policy enforcement any S/MIME-encrypted email
- Use financial services, healthcare, and other custom lexicons and filters to identify sensitive, inappropriate, and proprietary information before it leaves your network
- Validate digital signatures using the Online Certificate Status Protocol (OCSP), and enforce policy on digitally signed messages



Key Features & Benefits**Enterprise-grade capabilities**

MailGate supports comprehensive email security infrastructures for large enterprises

- An award-winning integrated administration dashboard, easy-to-implement clustering, and seamless integration into any environment means you can have MailGate up and running quickly
- Support for enterprise multi-tenancy allows you to apply different policies to different business units/departments with a single MailGate installation, reducing deployment and maintenance costs
- Support for IPv6 protects your investment as the public and private sectors move to adopt the new protocol

Comprehensive, flexible, and easy-to-manage email security

Axway MailGate provides multiple tiers of security that can be used individually or in combination to block threats at the DMZ and within the enterprise network, and secure inbound and outbound email traffic at the content and network levels. MailGate can seamlessly plug-and-play with your existing architecture with no browser or operating system dependencies, giving you the flexibility to add new levels of security as your needs change — without making changes to your enterprise systems, applications, protocols, or end-user workflows.

Centralized email security management

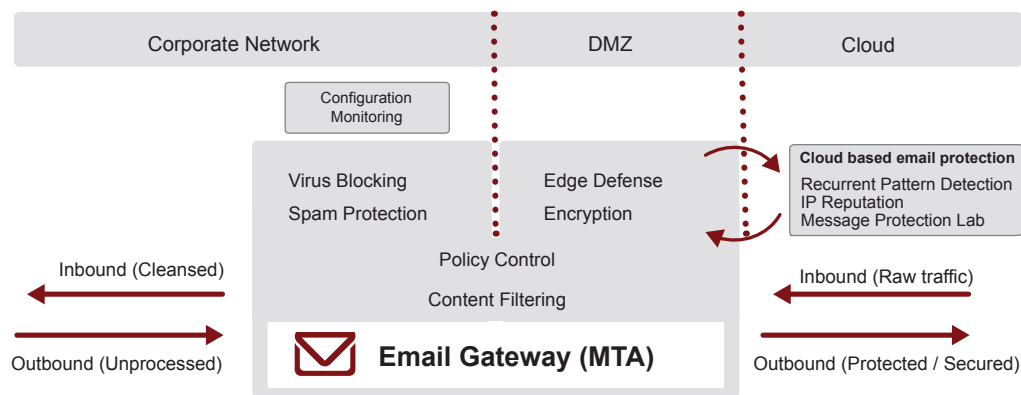
- Centralized management means you can have MailGate up and running quickly, processing close to two million messages per hour.
- A powerful management dashboard provides real-time visibility into email traffic, network attacks, spam statistics, message queues, content filtering, and more — even across multiple appliances or virtual environments.
- Automated report generation, data export for custom reporting, and advanced message tracking save time and improve visibility.

Antivirus

- Advanced Kaspersky and McAfee engines detect and strip viruses from all major file types, including mobile code and compressed file formats.
- Automatic virus definition and engine updates provide uninterrupted virus scanning, maximizing uptime and accelerating deployment of cures.
- Zero-hour protection quarantines suspicious messages and attachments in the critical early hours of a virus outbreak.
- Granular antivirus policies can be defined and enforced around users, recipients, attachment types, and executables.



Axway MailGate



Antispam

- Intelligent language-based technology recognizes spam like a human reader would, and prevents it from entering the network.
- Deploy enterprise-wide spam protection in 30 minutes or less to immediately eliminate more than 99% of spam — with a false-positive rate of only one in 100,000.
- Configurable filters and automatic spam-definition updates meet your unique requirements.

Intelligent Edge Defense

- Anomaly detection and rate throttling with real-time zombie detection and IP reputation services defend against distributed botnet attacks.
- Reduce raw email loads by more than 90% by eliminating directory harvest attacks, denial-of-service attacks, malformed SMTP packets, invalid recipient addresses, and other forms of malicious and invalid messages.
- Verify recipients at the perimeter to create IP-based block and allow lists, identify suspicious senders, and apply intelligent traffic shaping and message throttling for invalid messages.
- Domain Keys Identified Mail (DKIM) technology authenticates user email domains to ensure that senders are who they say they are.

Content Filtering

- Scan and analyze email content and more than 300 types of attachments, including multiple levels of embedded archive files and hidden document text.
- Set up simple checkbox filters to identify personal and financial data, including Social Security or personal identification numbers, banking/trading (CUSIP), and credit/debit card numbers.
- Use the financial services lexicon to scan for personal financial information, including statements, account numbers, PINs, and trade confirmations.
- Use the HIPAA lexicon to scan for PHI, including patient identifiers, medical diagnostics and procedures, drug names, and treatment phrases.



Delivery Options

- Hardened Linux Appliance
- Axway/Dell Appliance
 - Virtual VMware Appliance

Encryption

- Define policies that automate gateway-to-gateway email encryption for any remote domain.
- Enforce TLS or S/MIME connections with remote domains, hostnames, partner sites, or IP addresses.
- Receive automatic alerts on TLS attempts and failures.
- Add Axway Secure Messenger for a comprehensive encryption platform.

Digital Rights Management

- Convert sensitive Microsoft Office documents into password-protected PDF files.
- Disable certain functions — such as copy/paste, print, and edit — to preserve the integrity of document content.
- Include custom watermarks in PDFs.
- Remove metadata and edit outbound messages to comply with corporate policy.

All-inclusive Email Security

- Deploy Axway MailGate on a hardened IPv6-supported Linux appliance which includes Axway Secure Messenger, a powerful desktop-to-desktop email encryption platform, to solve all of your email security issues with a comprehensive solution on one appliance.
- License email hygiene and secure messaging separately or together. Enable both at once, or over time your organization grows.
- A single install wizard, single admin UI, and single end-user UI deliver enhanced ease-of-installation and ease-of-use.

High Availability/Disaster Recovery

- Utilize disaster recovery capabilities to survive a data or server catastrophe with email intact. Backed-up data can be restored.
- Use network-attached storage (NAS) to enable true application-based high availability, for seamless functionality in the event of system failure.