

Axway Secure Messenger

Protect your business with policy-based email encryption



No organization wants to end up in the news because of a data leak — especially an accidental leak of sensitive information that resulted from one employee sending an unsecured email or attachment to the wrong address. The costs of these kinds of security failures can be devastating — data loss, business disruption, damage to brands and reputations, as well as litigation and regulatory fines.

Axway Secure Messenger™ can shield your business from these threats by improving email security, governance and compliance. Combining a state-of-the-art SMTP relay with powerful policy-based content filtering, Secure Messenger inspects all incoming and outgoing email at the Internet gateway to identify email and file attachment content that is in violation of the enterprise security policies you define, and automatically redirects suspect messages to a secure channel for encrypted delivery, quarantine, deletion or other action. This perimeter-based approach ensures that all users — internal and external — comply with your enterprise policies all the time, without having to actively implement or manage encryption software on their desktops, or change their common usage patterns.

Key Features & Benefits

Comprehensive encryption capabilities

Secure inbound and outbound email communications, whether the channel is gateway-to-gateway, gateway-to-desktop or Web-based message delivery

- Encrypt and authenticate messages based on centralized policies and automated message routing
- Use email to deliver confidential information and corporate assets, and to document sensitive business transactions
- Deploy secure email capabilities to any employee, customer or partner — without requiring them to install or learn new software. Automatic gateway-to-gateway encryption requires no end user intervention at all

Powerful email policy management

Set and manage policies to analyze, manage, protect, track and report on email traffic flowing in and out of your organization

- Simple checkbox content filtering, an intuitive policy manager, and automatic gateway-to-gateway encryption make it easy to prevent accidental data leakage
- Leverage existing applications and networks with password enrollment and management services, and easy integration with third-party identity management systems
- Define and enforce messaging policy at the domain, group and individual levels



Key Features & Benefits**Simplified governance and regulatory compliance**

Specialized lexicons and enhanced scanning and tracking features make it easy to comply with evolving industry standards and government regulations

- Create content filters to identify personal information that is protected by laws such as the U.S. PCI Data Security Standard, European Union Data Protection Directive and Japanese Personal Data Protection Law
- A financial services lexicon scans messages and attachments for corporate and personal financial information to simplify compliance with SOX, GLBA and other regulations
- A HIPAA lexicon scans for protected health information (PHI) to enforce compliance with HITECH/HIPAA and other healthcare regulations
- Message delivery tracking all the way to recipient's desktop creates a documented "paper trail" for audit and compliance purposes

The industry's most accessible email data encryption solution

Because an enterprise typically cannot mandate special desktop software for sending or receiving secure email beyond its own network, Secure Messenger provides a range of message delivery methods that rely only on standard email clients and web browsers — there is no desktop software to install or manage.

Online pull delivery using a Web browser (Secure Webmail)

Secure Webmail uses a Web link embedded in an email message to route the recipient back to a secure server to read the message over a Web browser. This methodology leverages existing SSL encryption capabilities in the browser for secure message delivery, while supporting browser-based authentication methods to ensure that only the correct recipient sees the message.

Recipients can access their messages from anywhere on the Internet, and reply to messages using the same secure delivery channel. All users have a secure Web-based mailbox (Secure Inbox) that allows them to send, receive, sort, search, delete, save and organize messages from anywhere on the Internet.

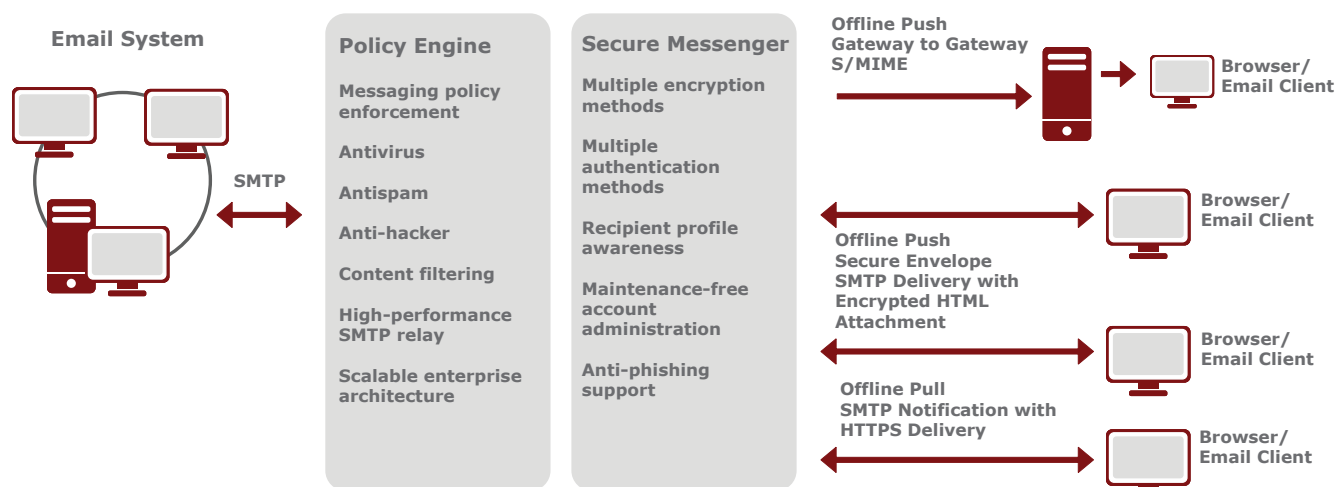
Offline push delivery using a Web browser (Secure Envelope)

Secure Envelope delivers an encrypted message directly to a recipient's email inbox using standard SMTP email as the transport, but includes encrypted message content in an HTML attachment. Recipients open the attachment using online or offline browsers, and enter a password to decrypt and read the message.

Gateway-to-gateway delivery using S/Mime

When a recipient organization's digital certificate is available for encryption and the organization's email infrastructure supports the S/MIME standard, Secure Messenger supports message delivery via gateway-to-gateway S/MIME encryption.





All-inclusive Email Security

- Deploy Axway Secure Messenger on a hardened IPv6-supported Linux appliance accompanied by Axway MailGate, an enterprise-grade inbound/outbound email hygiene manager, to solve all of your email security issues with a comprehensive solution on one appliance.
- License Secure Messenger and MailGate separately or together. Enable both at once or over time, as needed and as 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.

Learn More

To learn more about how Axway Secure Messenger can shield your business from data leak threats by improving email security, governance and compliance, email us at axwaysolutions@axway.com, or visit us at www.axway.com/contact-us.

Delivery Options

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

For More Information, visit www.axway.com

Copyright © Axway 2011. All rights reserved.

