Secure Messenger™

Intelligent, automated email encryption and policy-based routing

Leaders Quadrant of Gartner Magic Quadrant
for Email Encryption, 2007

Encrypt enterprise email for regulatory compliance, maximum security and policy enforcement with Secure Messenger, the industry's most comprehensive and flexible email encryption product.

Secure Messenger™ is an award-winning, industry-leading email encryption platform that enables you to protect, analyze, manage and report on email traffic flowing in and out of your organization. Whether your organization is striving to protect confidential information and intellectual property, comply with increasingly stringent government and industry regulations, meet the security demands of partners, suppliers and customers, or prevent email data leakage, you need powerful, easy-to-implement email encryption that doesn't require additional staff or disrupt established workflow. Secure Messenger's enterprise-class, component-based architecture includes a state-of-the-art SMTP relay and a powerful policy engine. It monitors messaging at the Internet gateway with a complete set of email security capabilities, and secures your inbound and outbound email streams. Secure Messenger provides an array of tools for encryption of email communications, whether the channel is gateway-to-gateway, gateway-to-desktop, or Web-based message delivery.

FLEXIBLE, POWERFUL ENCRYPTION CAPABILITIES

Secure Messenger can be configured to identify policy violations based on message content, and take an array of actions to prevent breaches of confidentiality. Secure Messenger protects sensitive communication and content by inspecting all incoming and outgoing messages based on policies you define. When an email is identified as potentially sensitive, it is flagged and sent to a recipient previously designated for secure, encrypted delivery. This feature ensures that all users comply with enterprise privacy and security policies each and every time they hit send. And Secure Messenger delivers this robust level of protection without software installs to the desktop and with no changes to the work practices of typical end users.

MULTIPLE SECURE MESSAGE DELIVERY OPTIONS

For secure business-to-consumer communications, Secure Messenger enables you to encrypt email at the desktop using patented "online pull" (Secure Webmail) and "offline push" (Secure Inbox®) technologies. Encrypted messages are delivered directly to a recipient's email inbox without requiring any special email client software or digital certificates to decrypt. Secure Webmail is based on Tumbleweed's patented staging server technology, which notifies a recipient of a message awaiting retrieval with an authenticated, encrypted Web link to a secure server.

FEATURES

– Secure email encryption

– Multiple Web and S/MIME delivery options

– Message tracking & auditing

– Policy-based encryption

– Deep content scanning capabilities

– Integrated dashboard admin

– Password self-management

– True message recall

– Works with any email server

– Directory integration

– Scalable enterprise architecture

– Branding toolkit

– 3 delivery models: hosted, appliance, software

BENEFITS

– Enforces enterprise messaging security policies for all internal and external users

– Ensures confidentiality and authentication for any user, regardless of messaging infrastructure

– Leverages existing investments in PKI and identity management solutions

– Automates and confirms delivery of sensitive information for compliance and auditing

– Requires no additional IT staff to manage users

Tumbleweed®
now merged with **Axway**

INDUSTRY-LEADING, POLICY-BASED ENCRYPTION

Secure Messenger's robust content filtering engine can scan any attribute of an email message, including its header, subject, message body or attachment. Depending on your industry needs, you can establish content policies to look for sensitive information such as Social Security numbers, private health information or corporate finance data. Our powerful, industry-specific lexicons and flexible pattern matching tools help you achieve compliance with a wide range of industry and government regulations. Secure Messenger can also identify intellectual property exiting your enterprise embedded in email messages and attachments.

For identity-based policies, Secure Messenger analyzes sender and recipient identities to determine whether message contents should be protected, and how. By integrating with existing enterprise directories, Secure Messenger can enforce messaging policy at the domain, group and individual level. To manage the complexities of user authentication for secure message delivery, Secure Messenger provides both its own password enrollment and management services, and integration with existing identity management systems. By providing content and identity awareness to your enterprise Internet email traffic, Secure Messenger determines when and how messages should be encrypted or otherwise secured.

A RANGE OF SECURE MESSAGE DELIVERY OPTIONS

Secure Messenger provides the industry's broadest array of proven secure email delivery methods. Because an enterprise typically cannot mandate special desktop software for sending or receiving secure email beyond its own network, Tumbleweed provides a range of delivery options that rely only on existing email client software and ubiquitous browser-based technologies.
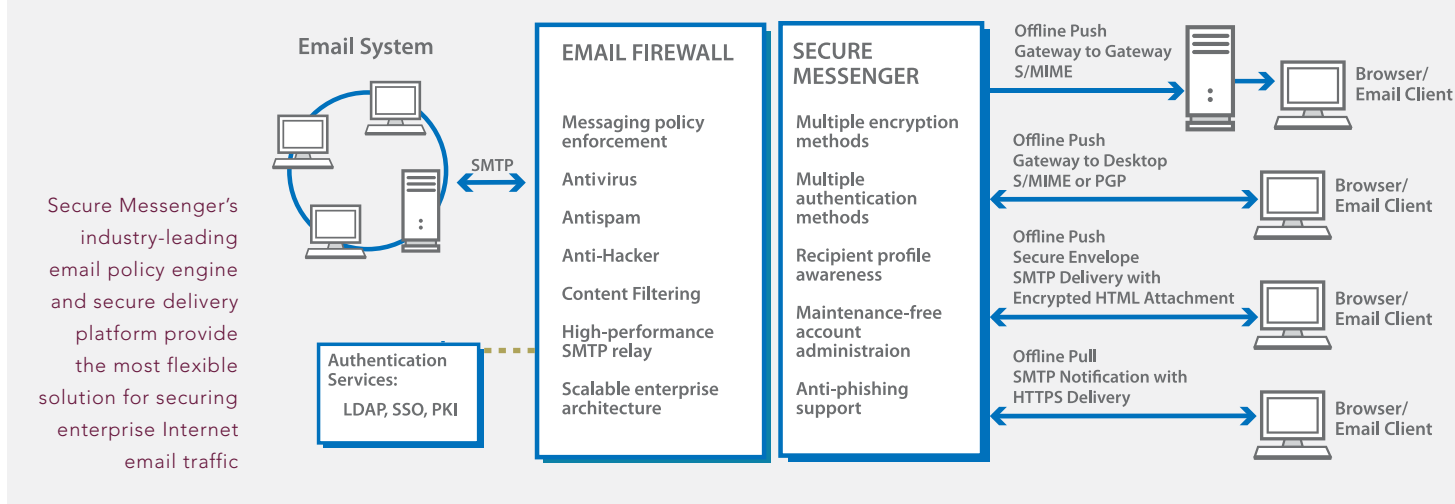
ONLINE PULL DELIVERY USING A WEB BROWSER (SECURE WEBMAIL)

Secure Webmail (online pull) uses a Web link embedded in an email message to route the recipient back to a secure server to read the message using a Web browser. Secure Webmail delivery allows recipients to receive, read, reply-to and locally save a secure message without any additional software plug-in or client-side software beyond their usual email clients and browsers. This methodology leverages existing SSL encryption capabilities in the browser for secure message delivery, while also supporting any browser-based authentication method 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 INBOX)

Secure Envelope (offline push) delivers an encrypted message directly to a recipient's email inbox, without requiring any special email client software or digital certificates to decrypt. Secure Envelope uses standard SMTP email as the transport, but includes the encrypted message contents in an HTML attachment. Recipients open the attachment using online or offline browsers, and enter a password in order to decrypt and read the message. Every Secure Envelope also includes a Web link that can direct users to a copy of the message on the server. This fallback option ensures that browser or system difficulties don't prevent recipients from reading their messages.

Tumbleweed Secure Messenger Architecture

Email System

Secure Messenger's industry-leading email policy engine and secure delivery platform provide the most flexible solution for securing enterprise Internet email traffic

SMTP

Authentication Services:
LDAP, SSO, PKI

EMAIL FIREWALL

Messaging policy enforcement

Antivirus

Antispam

Anti-Hacker

Content Filtering

High-performance SMTP relay

Scalable enterprise architecture

SECURE MESSENGER

Multiple encryption methods

Multiple authentication methods

Recipient profile awareness

Maintenance-free account administraion

Anti-phishing support

Offline Push Gateway to Gateway S/MIME — Browser/Email Client

Offline Push Gateway to Desktop S/MIME or PGP — Browser/Email Client

Offline Push Secure Envelope SMTP Delivery with Encrypted HTML Attachment — Browser/Email Client

Offline Pull SMTP Notification with HTTPS Delivery — Browser/Email Client

OFFLINE PUSH DELIVERY USING S/MIME

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

GATEWAY-TO-GATEWAY: If your organization and the receiving organization each have S/MIME-compatible email gateways, you can exchange secure email automatically. After an initial exchange of a single digital certificate, Secure Messenger transparently secures all future email between all users in the two enterprises using strong S/MIME encryption and digital signature technology. Tumbleweed's certification under the S/MIME Gateway (SMG) program ensures ongoing interoperability with other vendors' gateway S/MIME implementations.

GATEWAY-TO-DESKTOP: To facilitate secure communication with several external end-users who have digital certificate support in their email client, Secure Messenger supports dynamic public key lookup and validation of certificates from external directory servers. If the external user has previously sent a signed message to your organization, Secure Messenger will automatically harvest the correct certificate and use it to encrypt all future email for that user. End-user proxy certificates allow external users to send S/MIME encrypted messages to your enterprise users while enabling you to inspect the inbound messages for viruses or other inappropriate content. Gateway-to-Desktop S/MIME in Secure Messenger makes secure email transparent—end-users do not need to manage external recipients' certificates.

SYSTEM REQUIREMENTS

– Intel® Pentium® 4 or equivalent

– 20GB hard drive

– 2GB memory

OPERATING SYSTEM

– Microsoft® Windows® 2003 Server or Advanced Server

DATABASE

– Microsoft® SQL Server® 2005

WEB SERVER

– Third-party HTTPS reverse proxies supported for stronger security configuration in the DMZ

Tumbleweed Secure Messenger

MULTIPLE AUTHENTICATION SERVICES

Secure Messenger's S/MIME-based delivery methods use pre-existing recipient digital certificates to provide authentication. Certificate validation support (CRL, CDP, etc.) is provided to ensure that revoked certificates are not used. For secure delivery methods that leverage a Web browser, multiple options are available to provide recipient authentication services:

– Auto-enrollment functionality lets you enroll external users into a trusted identity management system managed by Secure Messenger. It provides administration-free password management functionality that enables end-users to create their own strong passwords, and password hints to aid recovery of forgotten passwords.

– A rich set of APIs provides integration capabilities with existing identity management systems. Whether based on LDAP, database or some other commercial authentication and authorization system, Secure Messenger's flexible APIs maximize your ability to authenticate users and minimize administration overhead.

Managing security services across all Internet email channels can be a complex task. User behavior, policy enforcement and technology interoperability are all factors that influence the success of any secure messaging deployment. With Secure Messenger, these factors can be controlled and centrally managed to provide the extensible secure messaging infrastructure that will enable business processes to be brought online swiftly and securely.

Secure Messenger is available on three delivery models to fit the unique needs and budget for your organization: hosted, appliance or software.

– Hosted – The most cost-effective and faster way to deploy Secure Messenger

– Appliances – Powerful out of the box on premise solution

– Software – Run Secure Messenger on your own preferred hardware platform

LEARN MORE TODAY

To learn more about how Tumbleweed's Secure Messenger can encrypt email for maximum security, policy enforcement and regulatory compliance, contact your regional office listed below, email us at info@tumbleweed.com, or visit us at www.tumbleweed.com
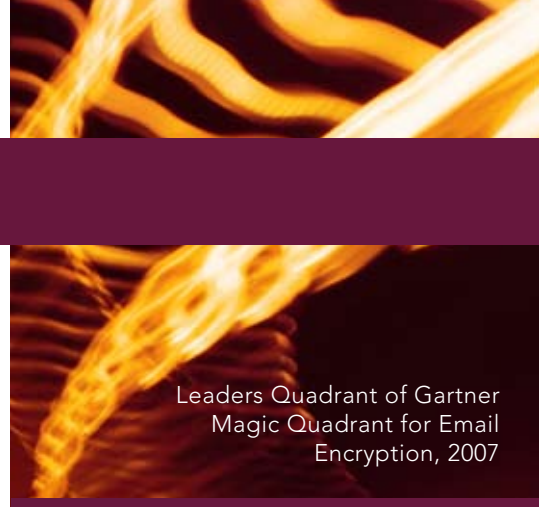
Leaders Quadrant of Gartner Magic Quadrant for Email Encryption, 2007

TUMBLEWEED PRODUCT LINES

Managed File Transfer
SecureTransport™ provides a centrally managed system for monitoring and managing secure file transfer activity across multiple file transfer sites or applications. SecureTransport integrates with the existing infrastructure and allows organizations to meet regulatory compliance mandates, and control and manage the transfer of files inside and outside of the corporate firewall.

Email Encryption
Secure Messenger™ is an email encryption platform that protects, analyzes, manages and reports on email traffic flowing in and out of the organization. Secure Messenger's enterprise-class, component-based architecture includes a state-of-the-art SMTP relay and a powerful policy engine. By monitoring messaging at the Internet gateway with a complete set of email security capabilities, Secure Messenger provides the most effective and reliable method to secure inbound and outbound email streams.

Email Security
MailGate® is a robust, easy-to-manage email security solution providing comprehensive inbound threat protection and outbound data loss prevention. Unrivaled antivirus, antispam, and Intelligent Edge Defense capabilities deflect junk email and inbound attacks, eliminating up to 90 percent of email traffic before it enters the network. MailGate's simple checkbox content filtering, an intuitive policy manager and automatic gateway-to-gateway encryption make it easy to prevent accidental data leakage.

Identity Validation
Validation Authority™ ensures the validity and integrity of highly valued and trusted transactions by validating digital certificates in real time. This comprehensive, scalable and reliable framework can validate certificates issued by any Certificate Authority.

Tumbleweed®
now merged with **Axway**

North America
Corporate Headquarters
1600 Seaport Blvd.
Suite 400, South Bldg.
Redwood City, CA 94063
Tel: 1-877-282-7390

Web: www.tumbleweed.com
E mail: info@tumbleweed.com

EMEA
Teal House, 2nd floor
3 Cowley Business Park
High Street, Cowley
Uxbridge
UB8 2AL
Tel: +44 (0) 1895 202 780

APAC
8 Shenton Way
#31-01 Temasek Tower
Singapore 068811
Tel: +65 6419 5486
Fax: +65 6777 3922