

 Tumbleweed MailGate Secure Messenger™

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

Every organization has unique security needs—from government privacy regulations in healthcare (HIPAA) to financial services (GLBA) and protection of corporate intellectual property to corporate governance (SOX). Tumbleweed MailGate Secure Messenger™ is the leading enterprise secure email software solution. This perimeter-based design guarantees that all users comply with enterprise security policies and saves you from installing software on every desktop. Secure Messenger identifies messages that require secure delivery based on a set of policies you define. It works with the Tumbleweed MailGate Email Firewall™ to inspect outbound email at the network gateway and automatically redirect messages that contain sensitive content to a secure, encrypted channel. It then applies the most appropriate delivery method for each recipient. Secure Messenger takes the burden of security decisions off the individual user, eliminating the need for training.

MULTIPLE SECURE MESSAGE DELIVERY OPTIONS

Secure delivery options include both Secure Envelope (offline push) and Staging Server (online pull) methods, to ensure ease of use and rapid adoption, regardless of what kind of computer systems users have on their desktops. The offline push methods deliver an encrypted message directly to a recipient's e-mail inbox without requiring any special e-mail client software or digital certificates to decrypt. The online pull method 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
- Multiple Web and S/MIME delivery methods
- Delivery tracking
- Policy-based encryption
- Password self-management
- Works with any email server
- Directory integration
- Scalable enterprise architecture
- Branding toolkit

BENEFITS

- Enforces enterprise messaging security policies for all internal and external users
- Delivers proven, usable security to ensure confidentiality and authentication for any user, regardless of their messaging infrastructure
- Leverages existing investments in PKI and identity management solutions
- Automates and confirms the delivery of sensitive information for compliance and auditing
- No additional IT staff required to manage users



"Tumbleweed provides the most comprehensive solution to both dynamically determine the presence of phi in our messaging traffic as well as choose the most appropriate method of secure delivery."

MARK WIESENBERG, DIRECTOR, STRATEGIC ARCHITECTURES
Sharp Healthcare

POLICY-BASED SECURE MESSAGE DELIVERY

MailGate Secure Messenger inspects incoming and outgoing Internet email to identify potentially sensitive correspondence based on a set of content and identity policies that you define. Once identified as likely to contain confidential information or addressed to a recipient whose email needs privacy, a message is automatically directed through a secure, encrypted message channel.

The robust content filtering engine in Secure Messenger can scan any attribute of an email message, including its header, subject, message body, or attachment. Depending on your needs, you can establish content policies to look for sensitive information like social security numbers, private health information, or corporate finance data using industry-specific lexicons and flexible pattern matching tools to comply with regulations like GLBA, HIPAA and SOX. Secure Messenger can also identify intellectual property leaving your enterprise embedded in email messages and attachments.

For identity-based policies, Secure Messenger analyzes the sender and recipient identities to determine whether message contents should be protected and how. By integrating with your 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 as well as 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 will be secured.

A RANGE OF SECURE MESSAGE DELIVERY OPTIONS

MailGate Secure Messenger provides the industry's broadest array of proven, usable secure email delivery methods in the market. 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 technology.

Email Notification Using Web Browser

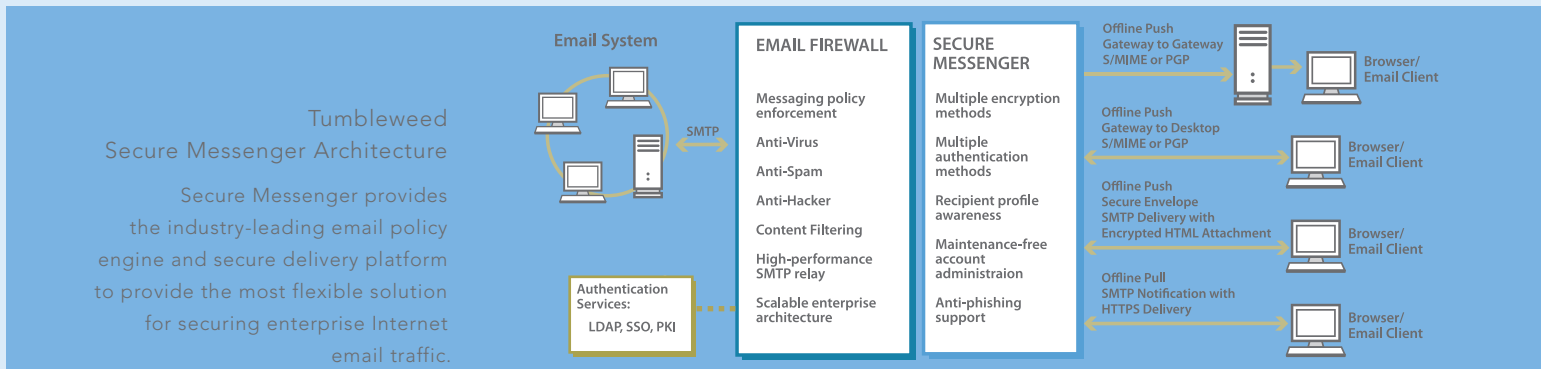
Tumbleweed's online pull secure delivery method (referred to as Email Notification) embeds a private Web link in an email notification to the user. Clicking on the link allows the recipient to access the message directly at a secure server with only one click after authentication. Email Notification allows recipients to receive, read, and reply to a secure message, as well as to save it—without the need for additional plug-ins or client-side software. This patented delivery method leverages existing SSL encryption capabilities in the user's browser for secure transport and also encrypts messages while stored on the server to provide the highest level of message protection.

By bringing recipients back to the enterprise Web site to read the message, the email notification method provides an integrated Web experience and centralized archive for all communications with customers and partners over the Internet.

Offline Push Delivery Using A Web Browser

MailGate Secure Messenger uses Secure Envelope™ technology to deliver 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 encapsulates the message content in an encrypted HTML attachment.

To decrypt and read a message, the recipient simply opens the attachment using their offline browser and enters a password. Because password entry and decryption functionality are embedded in the HTML attachment, the recipient's browser can manage the process without pre-installed software. Recipients can easily reply to the message using their browser once online. The offline push method allows message recipients to manage their secure communications with the enterprise, locally on their desktop.



Tumbleweed
Secure Messenger Architecture

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

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, MailGate Secure Messenger supports offline push delivery via both gateway-to-gateway and gateway-to-desktop S/MIME.

GATEWAY-TO-GATEWAY:

If your organization and the receiving organization each have S/MIME-compatible email gateways, such as the Email Firewall, 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 recent 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 server 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, because your end-users do not need to manage external recipients' certificates.

SYSTEM REQUIREMENTS

HARDWARE

- Intel® Pentium® 4 or equivalent
- 20GB hard drive
- 2GB memory

OPERATING SYSTEM

- Microsoft® Windows® 2000 Server or Advanced Server

DATABASE

- Microsoft® SQL Server 2000

WEB SERVER

- Administrator interfaces: Microsoft Internet Information Server 5.0 (integrated with the Email Firewall)
- End user interfaces: Jetty Web server included with the embedded JBOSS application server. Third party HTTPS reverse proxies supported for stronger security configuration in the DMZ

TUMBLEWEED INDUSTRIES

BANKING & FINANCE

ABN AMRO Bank
ADP
Alliance Data Systems
AXA Financial
Bear Stearns
Deutsche Bank
JPMorgan Chase
MasterCard
NASD Production Services
Wells Fargo Bank

GOVERNMENT ORGANIZATIONS

California Health and Human Services
Connecticut Dept. of Labor
LA Department of Mental Health
State of Washington
Singapore Central
Providence Fund
US Navy Surface Warfare Center

HEALTHCARE & INSURANCE

AdvancePCS
AON
Blue Cross Blue Shield of Florida
Group Health Cooperative
New York Life Insurance
WebMD Envoy

ENTERPRISES

General Motors
Johnson & Johnson
Sears Roebuck and Company
Symantec
Verizon

MULTIPLE AUTHENTICATION SERVICES

MailGate Secure Messenger delivery methods based on S/MIME use pre-existing recipient digital certificates to provide authentication. Certificate validation support (CRL, CDP, etc.) is provided to ensure 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 let you maximize your ability to authenticate users and minimize the 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 affect the success of any secure messaging deployment. With Secure Messenger, these factors can be controlled and centrally managed to provide the extendible secure messaging infrastructure that will enable more business processes to be brought online in a shorter time frame.

SECURE MESSENGER CUSTOMERS INCLUDE:

- Over 40% of Blue Cross & Blue Shield organizations
- Multiple regional healthcare provider networks
- Leading U.S. pharmaceutical companies
- Top brokerage services
- Leading online banking services
- Various insurance companies
- Federal and state government agencies
- Manufacturing firms
- International email and postal service providers

TUMBLEWEED PRODUCT LINES

Email Security

Protect your email network by blocking spam and viruses, encrypting and routing traffic, and filtering content with Tumbleweed MailGate™.

Managed File Transfer

Send and receive large files securely and efficiently, without the need for proprietary software or networks with Tumbleweed SecureTransport™.

Identity Validation

Ensure the validity and integrity of highly valuable and trusted transactions in real-time with Tumbleweed Validation Authority™.



California, USA
Corporate Headquarters
Tumbleweed Communications Corp.
700 Saginaw Drive
Redwood City, CA 94063

Phone: 650-216-2000/800-696-1978
www.tumbleweed.com

New York, USA
Tumbleweed Communications Corp.
245 Park Ave, 24th Floor
New York, NY 10167

Phone: 212-209-7363/800-696-1978
www.tumbleweed.com

United Kingdom
Tumbleweed Communications Ltd.
Hurst Grove, Sanford Lane
Hurst, Berkshire RG10 0SQ
UK

Phone: +44 (0)118 934 7100
www.tumbleweed.com

APAC
Tumbleweed Communications
Centennial Tower, Level 21
3 Temasek Avenue
Singapore 039190

Phone: 65-65497143
www.tumbleweed.com

© 2006 Tumbleweed Communications Corp. All rights reserved. Tumbleweed is a registered trademark and Tumbleweed SecureTransport, SecureTransport Server, SecureTransport Edge, Tumbleweed MailGate, and Tumbleweed Validation Authority are trademarks of Tumbleweed Communications Corp. All other brand names are the trademarks of their respective owners. 03/06