ASK technologies, inc.
www.asktech.com

Tumbleweeds Secure Messenger Overview

Tumbleweed®
now merged with Axway

Tumbleweeds Secure Messenger leads the industry as an email encryption service that allows you to analyze, encrypt, manage, and report on your organization's emails coming inbound and outbound. There are several reasons why people turn to Tumbleweeds Secure Manager:

- Protect Confidential Information or Intellectual Property
- Protect against Identity Theft (Encrypting SSN or Passwords)
- Comply with Government or Industry Auditing and Regulations (ex. Medical and Financial Fields)
- Rise above the security expectations of your partners, customers, and staff

Increasingly data theft and online theft is an extraordinary problem. Tumbleweeds is a powerful, fast, and easy to integrate email encryption system. It monitors and secures both your incoming and outgoing emails.

FEATURES

☐ Secure email encryption

☐ Multiple Web and S/MIME delivery options

☐ Message tracking & auditing

☐ Policy-based encryption

☐ Deep content scanning capabilities

☐ Password self-management

☐ True message recall

☐ Scalable enterprise architecture

Tumbleweeds Secure Messenger
Overview

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

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. 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 communication.

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.

ASK technologies, inc.
www.asktech.com

Tumbleweeds Secure Messenger Overview

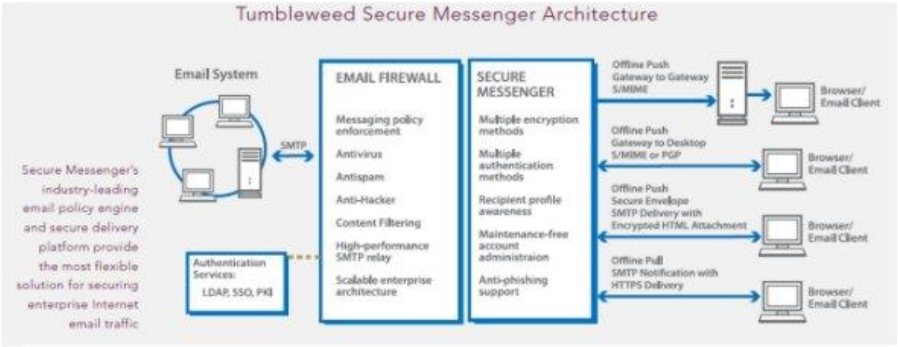
INDUSTRY-LEADING, POLICY-BASED ENCRYPTION

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.

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.



Click the picture for larger version.

ASK technologies, inc.
www.asktech.com

Tumbleweeds Secure Messenger Overview

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.