

Axway Secure Messenger

Protégez votre entreprise avec le cryptage du courrier électronique basé sur des règles



Aucune entreprise ne souhaite faire les gros titres à cause d'une fuite de données, en particulier une fuite accidentelle d'informations sensibles provoquée par l'envoi d'un courrier électronique ou d'une pièce jointe non sécurisés par un employé à une mauvaise adresse. Les coûts de ces types de failles de sécurité risquent de s'avérer dévastateurs : perte de données, interruption d'activité, atteinte à l'image de marque de l'entreprise ou frais de litige et amendes réglementaires.

Axway Secure Messenger™ peut protéger votre entreprise de ces menaces en améliorant la sécurité, la gouvernance et la conformité du courrier électronique. Alliant un relais SMTP hors pair à un filtrage performant du contenu basé sur des règles, Secure Messenger inspecte chaque message électronique entrant et sortant au niveau de la passerelle Internet. Il identifie ainsi le contenu du courrier et des pièces jointes non conformes aux politiques de sécurité définies par l'entreprise et redirige automatiquement les messages suspects vers un canal sécurisé pour une remise chiffrée, une mise en quarantaine, une suppression ou toute autre action. Cette méthode de type périmétrique garantit que tous les utilisateurs, internes et externes, respectent en permanence les politiques de l'entreprise, sans nécessité de mettre activement en œuvre ou de gérer un logiciel de cryptage sur leurs postes de travail, ni de modifier leurs modes d'utilisation courants.

Fonctionnalités clés et avantages

Fonctionnalités complètes de cryptage

Messages électroniques entrants et sortants sécurisés, que le canal soit de passerelle à passerelle, de la passerelle au poste de travail ou une remise de message sur le Web.

- Crypter et authentifier les messages selon des règles centralisées et un routage des messages automatisé.
- Utiliser le courrier électronique pour livrer des informations confidentielles et des actifs d'entreprise, ainsi que pour documenter des transactions métier sensibles.
- Déployer des fonctions de messagerie sécurisée pour tout employé, client ou partenaire, sans lui demander d'installer ou d'apprendre à utiliser un nouveau logiciel. Un cryptage de passerelle à passerelle ne requiert aucune intervention de l'utilisateur final.

Fonctionnalités clés et avantages	
<p>Gestion efficace des règles de courrier électronique Définissez et gérez des politiques pour analyser, gérer, protéger, suivre et produire des rapports sur le trafic de courrier électronique reçu et envoyé à votre entreprise.</p>	<ul style="list-style-type: none"> ▪ Filtrage du contenu à l'aide d'options simples, gestion intuitive des règles et cryptage automatique de passerelle à passerelle pour faciliter la prévention des fuites de données accidentelles. ▪ Tirer parti des applications et réseaux existants grâce à des services d'inscription de mots de passe et d'administration, ainsi qu'une intégration facile à des systèmes de gestion d'identité tiers. ▪ Définir et appliquer des règles de messagerie au niveau domaine, groupe et utilisateur.
<p>Gouvernance simplifiée et conformité réglementaire Des lexiques spécialisés et des fonctionnalités avancées d'analyse et de suivi simplifient la conformité aux normes sectorielles et réglementations administratives en constante évolution.</p>	<ul style="list-style-type: none"> ▪ Créer des filtres de contenu pour identifier les informations personnelles protégées par des lois telles que la loi américaine PCI Data Security Standard, la directive européenne sur la protection des données et la loi japonaise sur la protection des données personnelles. ▪ Un lexique Services financiers analyse les messages et les pièces jointes pour détecter les données financières d'entreprise et personnelles, afin de simplifier la conformité aux normes SOX, GLBA et autres réglementations. ▪ Un lexique HIPAA analyse les informations protégées relatives à la santé pour assurer la conformité aux normes HITECH/HIPAA et autres réglementations de santé. ▪ Le suivi de la remise des messages à chaque étape jusqu'au poste de travail du destinataire crée une trace documentaire à des fins de conformité et d'audit.

La solution de cryptage des données du courrier électronique la plus accessible du marché

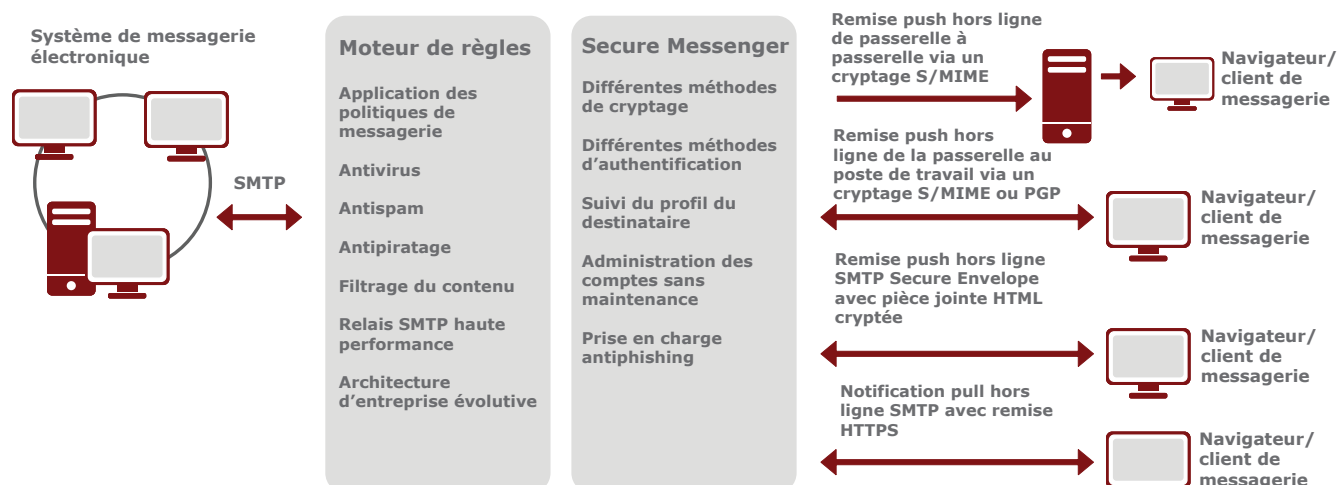
Parce qu'une entreprise ne peut généralement pas demander un logiciel de poste de travail particulier pour l'envoi ou la réception de messages électroniques sécurisés au-delà de son propre réseau, Secure Messenger propose un ensemble de méthodes de remise de messages qui ne s'appuie que sur des clients de messagerie standard et des navigateurs Web. Nul besoin d'installer ou de gérer un logiciel sur le poste de travail.

Remise pull en ligne à l'aide d'un navigateur Web (Secure Webmail)

Secure Webmail utilise un lien Internet intégré dans un message électronique pour rediriger le destinataire vers un serveur sécurisé afin de lire le message via un navigateur Web. Cette méthode exploite les fonctionnalités existantes de cryptage SSL sur le navigateur pour une remise sécurisée des messages, tout en prenant en charge une procédure d'authentification sur le navigateur pour s'assurer que seul le bon destinataire lise le message.

Les destinataires peuvent accéder à leurs messages de n'importe où sur Internet et y répondre en utilisant le même canal de distribution sécurisé. Chaque utilisateur dispose d'une messagerie sécurisée sur le Web (Secure Inbox) qui leur permet d'envoyer, de recevoir, trier, rechercher, supprimer, enregistrer et organiser les messages de n'importe où sur Internet.





Remise pull hors ligne à l'aide d'un navigateur Web (Secure Envelope)

Secure Envelope remet un message crypté directement dans la messagerie Web du destinataire sous forme d'un courrier électronique SMTP standard, mais intègre du contenu de message crypté dans une pièce jointe HTML. Les destinataires ouvrent la pièce jointe grâce à des navigateurs en ligne ou hors ligne, puis saisissent un mot de passe pour décrypter et lire le message.

Remise push hors ligne à l'aide du cryptage S/MIME

Lorsque le certificat numérique d'un destinataire peut être crypté et que l'infrastructure de messagerie du destinataire prend en charge la norme S/MIME, Secure Messenger assure la remise push hors ligne via un cryptage S/MIME de passerelle à passerelle et de la passerelle au poste de travail.

Sécurité complète du courrier électronique

- Déployez Axway Secure Messenger sur une appliance Linux renforcée et prise en charge par le protocole IPv6 ainsi qu'Axway MailGate, une solution de protection du courrier électronique entrant et sortant, haut de gamme, afin de résoudre tous vos problèmes de sécurité du courrier électronique avec une solution complète unique sur une seule appliance.
- Obtenez des licences pour Secure Messenger et MailGate séparément ou en même temps. Déployez les deux solutions en même temps ou l'une après l'autre, selon vos besoins et l'évolution de votre entreprise.
- Un seul assistant d'installation, une seule interface d'administration et une seule interface utilisateur offrent une facilité d'installation et d'utilisation.

Options de déploiement

- Appliance Linux renforcée
- Appliance Axway/Dell
 - Appliance virtuelle VMware

Haute disponibilité/Reprise d'activité

- Utilisez des fonctionnalités de reprise d'activité en cas de problème de données ou de serveur, avec un courrier électronique intact. Il est possible de restaurer les données sauvegardées.
- Utilisez un serveur de stockage NAS (Network Attached Storage) pour permettre une haute disponibilité réelle orientée application, pour une fonctionnalité transparente en cas de panne système.

En savoir plus

Pour découvrir comment Axway Secure Messenger peut protéger votre entreprise contre les menaces de fuites de données en renforçant la sécurité, la gouvernance et la conformité du courrier électronique, écrivez-nous à l'adresse axwaysolutions@axway.com ou rendez-nous visite sur le site www.axway.fr/contactez-nous.