clearswift
RUAG Cyber Security

Clearswift SECURE Email Gateway

Le courrier électronique restant le principal outil de collaboration professionnel, les entreprises doivent s'assurer que le contenu et l'information qu'elles envoient et reçoivent par ce canal sont appropriés et autorisés à entrer dans ou quitter l'entreprise. La solution Clearswift SECURE Email Gateway (SEG) sécurise contre la fuite d'informations critiques et protège la propriété intellectuelle et la réputation de votre entreprise tout en garantissant sa conformité aux réglementations et normes en vigueur.

Les fonctionnalités primées d'inspection en profondeur du contenu de Clearswift offrent les avantages concurrentiels propres aux communications ouvertes et fiables en transformant le courrier électronique d'un canal de communication à haut risque en un canal sur mesure capable de répondre aux besoins de votre entreprise. La passerelle analyse le contenu sensible présent dans les emails et fournit à partir d'une politique organisationnelle granulaire, la souplesse nécessaire pour autoriser différents comportements en fonction de l'expéditeur et du destinataire du message. La fonctionnalité d'anonymisation contextuelle de Clearswift modifie le contenu de manière dynamique pour le rendre fiable plutôt que de devoir stopper et bloquer le message et contraindre à une remédiation.

Protection contre les menaces entrantes

Comprend les solutions antivirus Kaspersky et/ou Sophos intégrées via le Cloud avec mise à jour automatique toutes les 15 minutes pour garantir la meilleure protection. Ces technologies sont complétées par une fonctionnalité de détection des malware Zéro-Hour et des codes actifs pour qu'aucun malware ne puisse pénétrer, ou sortir, via le courrier électronique. Les attaques ciblées utilisent généralement un email associé à des fichiers Office et PDF couramment utilisés comme vecteur d'envoi de charge utile. Si ces charges utiles parviennent à atteindre le poste de travail, elles seront exécutées avec les privilèges utilisateur du destinataire, ce qui pourrait faciliter l'accès à des données sensibles. Aussi, en complément de fonctionnalités anti-malware standard, la fonctionnalité de suppression des codes actifs supprime les macros, scripts et codes Active X des messages et des fichiers PDF et Office pour réduire considérablement le taux de réussite des attaques ciblées. Le nettoyage des messages permet de supprimer les URL, les pièces jointes et le code HTML des messages pour éradiquer tout risque potentiel lié à ces messages.

Détection des spams à la pointe du marché

La nouvelle passerelle Clearswift SECURE Email Gateway fournit un moteur anti-spam complètement refondu qui intègre le composant de pointe Mailshell. Ainsi, le volume de spam à destination des utilisateurs ainsi que le nombre de faux positifs s'en trouvent réduits. Le support des protocoles DMARC, SPF et DKIM permet de réduire encore plus le spam tandis que le plugin Spam Reporter pour Outlook permet de surveiller, consigner et éliminer le spam. Intégrant un nouveau mécanisme de défense multiniveau contre le spam à l'aide de systèmes de réputation des adresses IP, de "greylisting", de signatures, d'analyse SPF, de listes noires RBL, d'authentification du destinataire et de moteurs d'apprentissage (bayésien) pour garantir des taux de détection supérieurs à 99,9%, la passerelle SEG réduit considérablement le temps que les utilisateurs passent à gérer leur messagerie ainsi que l'effet du malware contenu dans le spam.

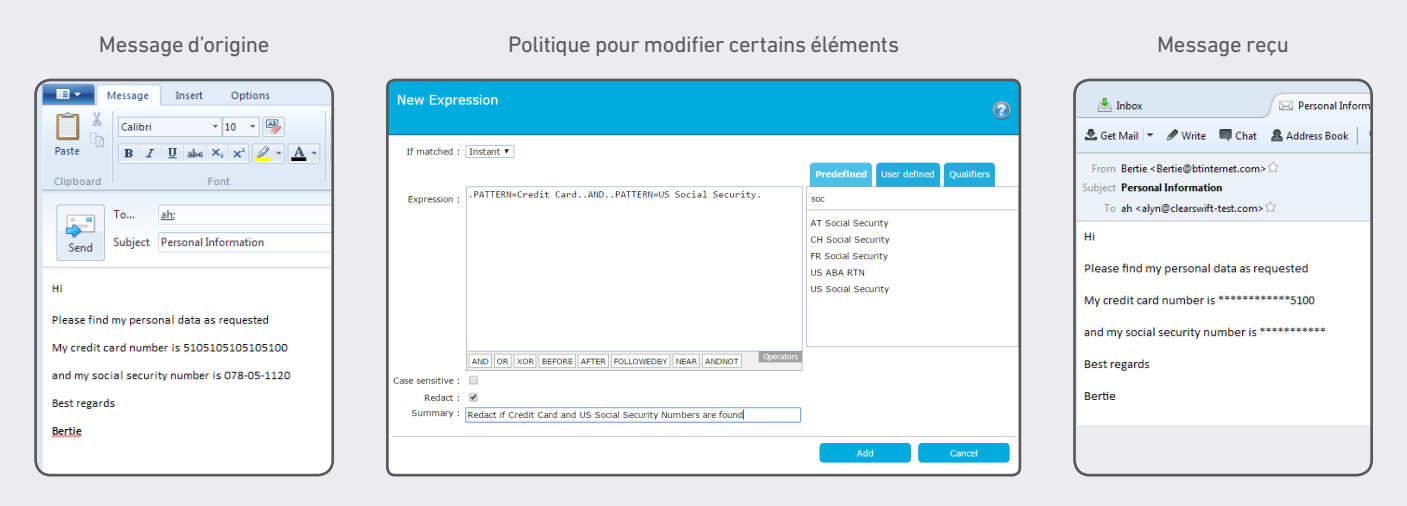
Politiques d'inspection contextuelle du contenu

Des politiques souples pour une inspection contextuelle du contenu vous évitent de devoir choisir entre des communications hors de contrôle et un risque inacceptable pour votre entreprise. Les politiques souples sont au cœur de tout déploiement concret. En effet, si une politique est trop restrictive, elle empêche les collaborateurs de travailler efficacement ou les oblige à trouver des moyens pour contourner la politique déployée.

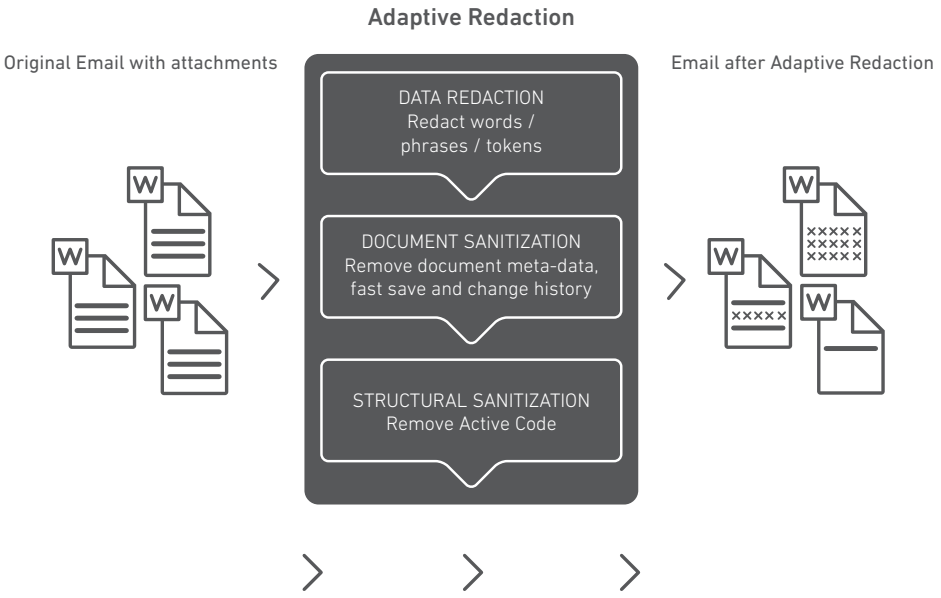
Anonymisation contextuelle

Les fonctionnalités d'anonymisation contextuelle uniques de Clearswift (Adaptive Redaction) permettent de modifier le contenu des messages et des pièces jointes de manière dynamique et à partir d'une politique. Grâce à la fonctionnalité d'anonymisation des données, l'information circule tandis qu'elle était auparavant bloquée. Il est possible de créer des politiques qui modifient des termes et des expressions spécifiques au sein des messages et des documents au moyen d'astérisques qui rendent le contenu fiable. Cette stratégie peut également s'appliquer aux numéros de cartes de crédit, numéros de sécurité sociale, noms de code d'un projet, noms de personnes ou tout autre information ayant une valeur particulière.

Figure 1. Anonymisation contextuelle Clearswift: anonymisation des données



Grâce à la fonctionnalité de suppression des métadonnées, vous pouvez supprimer les révisions en cours et nettoyer les données d'historique et de sauvegarde rapide qui peuvent contenir des informations critiques embarrassantes si elles sont divulguées par accident. Les propriétés d'un document telles que "l'Auteur", "l'Entreprise" et "le statut" peuvent être totalement supprimées ou être préservées pour certaines.



Prévention contextuelle des fuites de données

Les fuites de données sont désormais au cœur des préoccupations des entreprises. Qu'il s'agisse des toutes dernières maquettes, de données clients ou d'informations privées sur un employé, la fuite de propriété intellectuelle peut ruiner une entreprise tant au niveau financier que réputationnel.

Afin de réduire les risques de perte accidentelle de données, la solution SECURE Email Gateway contrôle les messages en fonction de leur contenu et de leur contexte. Le contexte est fourni via l'intégration à Active Directory ou LDAP pour appliquer une politique à un individu ou un groupe spécifique (ou à l'ensemble de l'entreprise). Quant au contenu du message, il est intégralement vérifié via plus de 90 politiques prédéfinies qui recherchent du texte spécifique dans le corps du message, dans le champ Objet et dans les pièces jointes.

Les politiques sont composées de termes et phrases standard ou d'expressions régulièrement utilisées qui servent à rechercher des caractéristiques alphanumériques complexes. En effet, ces dernières pourraient servir à identifier les actifs d'une entreprise, notamment les numéros de carte de crédit, d'IBAN, de sécurité sociale, etc.

Ces expressions peuvent être associées à l'aide d'opérateurs booléens et positionnels pour créer des exemples ayant notamment trait à une carte de crédit ou un projet ou un support confidentiel :

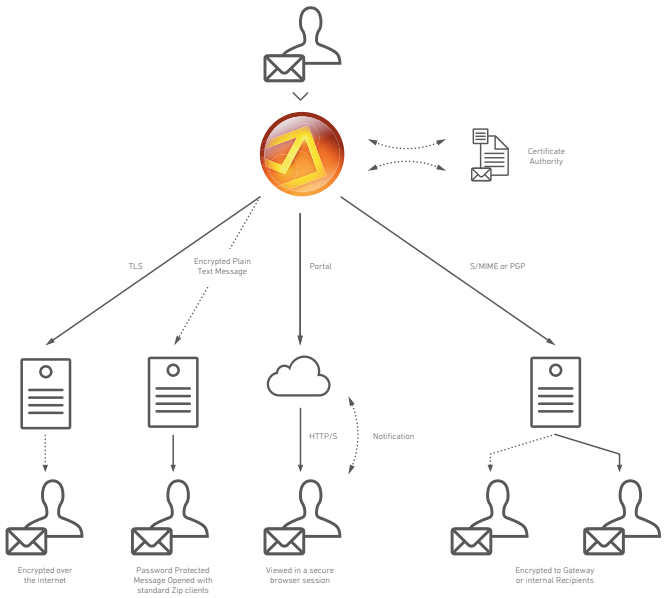
- Credit .FOLLOWEDBY=1. Card
- Confidential .AND. (Project .OR. Material)

Conformité

Se conformer à la réglementation est très important. Pour vous y aider, la passerelle SECURE Email Gateway fournit des modèles standards ainsi que des dictionnaires pour les termes courants pouvant indiquer une fuite de données.

Les passerelles sont fournies avec des dictionnaires personnalisables pour GLBA, HIPAA, SEC et SOX afin d'accélérer le déploiement. Les entreprises qui doivent se conformer aux réglementations portant sur les cartes de paiement (PCI) et les informations personnellement identifiables (IPI) peuvent s'appuyer sur un dictionnaire personnalisé et des jetons "carte de crédit" et "sécurité sociale" spéciaux. Il est toujours possible d'enrichir les dictionnaires standards avec d'autres dictionnaires plus spécialisés.

Comme il faudra toujours partager certaines informations, le chiffrement du courrier électronique est une autre fonctionnalité majeure de la passerelle pour garantir à l'aide d'un chiffrement puissant le respect de la règlementation relative aux données sensibles transmises via Internet. La loi HITECH américaine et la loi britannique sur la protection des données stipulent clairement que les données sensibles doivent être chiffrées lors de leur transmission par courrier électronique. La solution SECURE Email Gateway prend en charge différents mécanismes de chiffrement pour fournir toute la souplesse requise.



Chiffrement du courrier électronique

Avec le protocole TLS en standard et des modes de chiffrement S/MIME, PGP, par mot de passe ou via un portail Web, la solution SECURE Email Gateway offre tout un éventail d'options pour répondre aux besoins des entreprises. Quelle que soit la solution retenue, la passerelle achemine les données sensibles en toute sécurité et en quelques secondes seulement et dans le meilleur format pour le destinataire.

Administration et reporting

L'interface utilisateur de la passerelle est à la fois puissante et conviviale. Grâce à des ressources d'administration à base de profils, d'automatisation et de réutilisation des politiques, il est rapide et simple de créer une politique, de gérer les violations, de suivre les messages et de signaler des tendances et des comportements. Des informations importantes sont ainsi communiquées sans consommer de précieuses ressources d'administration.

Inspection du contenu en profondeur

Une véritable détection du type de fichier qui reconnaît les fichiers d'après leur signature et non pas selon leur extension permet à la passerelle Clearswift SECURE Email Gateway de reconnaître les fichiers avec précision. Les archives de fichiers compressés sont ouvertes et le contenu est examiné en temps réel. Les documents imbriqués sont découverts et le contenu est analysé en profondeur pour vérifier qu'il n'y a aucun risque de fuite de données.

Options de déploiement souple

C'est vous qui décidez du mode d'acquisition et de déploiement de la solution Clearswift SECURE Email Gateway, que ce soit sous la forme d'une appliance matérielle pré-installée, d'une image logicielle pouvant être chargée sur un éventail de plateformes matérielles ou encore d'une appliance virtuelle dans un environnement VMware / HyperV. Clearswift SECURE Email Gateway est également disponible en tant que solution Cloud via des fournisseurs tels qu'AWS et Azure ou directement auprès de Clearswift (offres régionales uniquement) sous la forme de serveurs virtuels hébergés qui vous permettent de garder le contrôle de la plate-forme avec tous les avantages et la commodité d'un modèle de fourniture dans le Cloud.

À propos de Clearswift

Clearswift permet à de nombreuses entreprises à travers le monde de protéger leurs informations sensibles afin qu'elles puissent collaborer en toute sécurité et développer leur activité. Notre technologie unique est une solution de prévention des fuites de données simple et 'contextuelle' qui limite le risque d'interruption de l'activité tout en permettant aux entreprises d'avoir une visibilité à 100% sur leurs informations critiques à tout moment.

Clearswift est présent dans le monde entier grâce à des sièges régionaux en Europe, Asie-Pacifique et aux États-Unis. Clearswift anime un réseau de partenaires de plus de 900 revendeurs à travers la planète.

Plus d'informations sur
www.clearswift.fr

Royaume-Uni - Siège international
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale, Reading, Berkshire
United Kingdom
RG7 4SA

Tél: +44 (0) 118 903 8903
Fax: +44 (0) 118 903 9000
Ventes: +44 (0) 118 903 8700
Support technique: +44 (0) 118 903 8200
Email: info@clearswift.com

Australie
Clearswift (Asie/Pacifique) Pty Ltd
Level 17 Regus
Coca Cola Place
40 Mount Street
North Sydney
NSW 2060
Australie

Tél: +61 2 9424 1200
Support technique: +61 2 9424 1210
Email: info@clearswift.com.au

Allemagne
Im Mediapark 8
D-50670 Cologne
Germany

Tél: ++49 (0) 221 8282 9888
Support technique: +49 (0) 221 8282 9886
Email: info@clearswift.de

Japon
Clearswift K.K
Shinjuku Park Tower N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo
163-1030
Japon

Tél: +81 (3)5326 3470
Support technique: 0800 100 0006
Email: info.jp@clearswift.com

États-Unis
Clearswift Corporation
309 Fellowship Road,
Suite 200, Mount Laurel,
NJ 08054
États-Unis

Tél: +1 856-359-2360
Support technique: +1 856 359 2170
Email: info@us.clearswift.com

Fonctionnalités	Avantages
Politique souple	
Contrôles granulaires des politiques	Définition facile à l'aide de politiques auto-documentées pour autoriser une utilisation avec un minimum de risques.
Intégration à un annuaire	Collecte régulière d'adresses électroniques d'expéditeurs et de destinataires à partir d'annuaires centralisés et d'informations sur la hiérarchie dans l'entreprise.
Politique souple	Création d'un workflow dédié aux messages électroniques nécessitant à un supérieur hiérarchique de les valider et de les relâcher afin de fournir un contexte plus riche au contrôle des messages.
Menaces entrantes	
Antivirus avec recherche assistée dans le Cloud et analyses heuristiques et comportementales	Interception d'infections dues à des malware connus et inconnus qui pénètrent ou quittent le réseau avec le choix entre 2 moteurs (Sophos et/ou Kaspersky).
Antimalware Zéro Heure	Détection et blocage de nouvelles attaques avant la mise à disposition des signatures virales pour réduire les risques liés à de nouvelles souches de malware.
Anti-spam multiniveau	Approche holistique de la détection des spams avec de nombreux moteurs antispam pour une détection supérieure à 99,9% avec un taux de faux positifs de 1 sur 300 000.
Suppression des codes actifs*	Suppression du code actif dans les fichiers Microsoft Office, Open Office et PDF pour leur transmission en toute sécurité plutôt qu'une simple détection du code actif présent sous la forme de macros, scripts et contrôles Active X dans les messages et les pièces jointes.
Nettoyage des messages	Suppression d'éléments représentant une menace potentielle dans le corps du message, par exemple des URL, du code actif et HTML.
Analyse d'images pornographiques	Analyse et mise en quarantaine des images avec du contenu pornographique pour réduire le risque d'offense aux destinataires.
Protection contre les fuites de données	
Identification des fichiers de type binaire	Identification précise basée sur une signature avec possibilité de définir ses propres signatures de fichiers.
Anonymisation contextuelle*	Suppression des termes et expressions sensibles que contiennent les messages et les pièces jointes. La suppression des métadonnées permet quant à elle de supprimer les propriétés, les marques de révision et les données de sauvegarde rapide dans un document.
Analyse lexicale et règles pour les expressions courantes	Recherche de mots-clés et d'expressions dans le contenu des fichiers en faisant correspondre une expression simple ou des caractéristiques plus complexes avec des expressions courantes pour identifier des données sensibles.
Politiques prédéfinies	Identification et détection aisées des jetons d'information standard, notamment les numéros de carte de crédit, de compte bancaire, de sécurité sociale et de pièces d'identité. La création et l'utilisation de politiques utilisateurs sont aisées.
Règles de workflow	Méthode pour assurer qu'un supérieur hiérarchique reçoive une copie des messages. Les messages contrevenant aux politiques sont gérés par un supérieur hiérarchique et leur envoi peut être différé le temps de les supprimer avant qu'ils ne sortent de l'entreprise.
Conformité	
Dictionnaires de conformité	Dictionnaires multilingues d'injures et de conformité éditables et qui supportent GLBA, HIPAA, SEC, SOX, PCI et IPI pour réduire au minimum les risques réputationnels et terminologiques.
Chiffrement intégré	Envoi de messages en toute sécurité via le protocole TLS fourni en standard avec des méthodes de protection S/MIME, PGP et par mot de passe* en option.
Chiffrement via un portail*	Chiffrement du courrier électronique via un portail Web pour envoyer des messages chiffrés à des utilisateurs non-techniciens.
Support de l'archivage vers serveur tiers	Options Relais vers et CCI pour transférer des copies de tous ou certains messages vers une solution d'archivage sur site ou dans le Cloud.
Administration	
Interface Web intuitive	Facilité d'utilisation sans aucun apprentissage nécessaire de syntaxe complexe ou de commandes Linux.
Reporting consolidé multi-passerelle	Vue consolidée du reporting des activités pour faciliter l'analyse et le partage de données d'administration.
Suivi des messages multi-passerelle	Vue de la provenance des messages, de leur traitement et de leur parcours via de multiples passerelles et fonctionnalité d'exportation manuelle ou programmée.
Alertes SYSLOG, SNMP, SMTP centralisées	Consolidation dans un système centralisé de gestion des événements et des informations de sécurité (SIEM) ou recours à des alertes d'administration SNMP ou SMTP.

clearswift
RUAG Cyber Security

*option tarifee