clearswift
RUAG Cyber Security

Clearswift SECURE Web Gateway

Internet peut désormais être considéré comme une extension de l'infrastructure de l'entreprise. Avec l'adoption croissante de services dans le Cloud tels que Salesforce.com et Office365 ainsi que l'utilisation d'Internet au travail par leurs collaborateurs, les entreprises doivent s'assurer que le contenu et les informations disponibles et consultées en ligne sont à la fois appropriés et autorisés par les politiques en place. Il est primordial de se protéger contre toute fuite de données critiques pouvant entraîner de sérieuses pénalités financières ou une atteinte à la réputation de l'entreprise. Clearswift SECURE Web Gateway (SWG) est une solution proactive de passerelle contrôlée par des politiques et qui transforme le Web d'un environnement à haut risque en une ressource fiable et adaptée aux besoins spécifiques de votre entreprise.

Les fonctionnalités primées d'inspection approfondie du contenu de Clearswift offrent les avantages concurrentiels inhérents aux communications ouvertes et fiables. La passerelle ne se contente pas uniquement de maintenir votre réseau à l'abri de virus, contenus inappropriés et exécutables dangereux. En outre, elle fournit un contrôle granulaire et complet de l'information consultée ou partagée en ligne, que ce soit pour limiter ou surveiller la navigation récréationnelle ou pour prévenir la fuite d'informations critiques. Grâce à la solution Clearswift SECURE Web Gateway, l'entreprise profite de tous les avantages offerts par les technologies Web 2.0 collaboratives. En effet, la fonctionnalité d'anonymisation contextuelle unique de Clearswift modifie le contenu de manière dynamique pour le rendre fiable plutôt que de devoir stopper et bloquer la communication, ce qui constitue une approche contextuelle de la protection des informations critiques.

Prévention des fuites de données

Grâce aux ressources d'analyse lexicales de la solution SECURE Web Gateway, il est possible de détecter et de prévenir les fuites de données accidentelles, l'un des fléaux que redoutent actuellement les entreprises. Qui plus est, les documents en cours de téléchargement peuvent être débarrassés des informations cachées dans les métadonnées. Que ce soit en recherchant des repères clés dans les documents téléchargés qui indiquent la présence de données sensibles ou en analysant le contenu, la fuite peut être identifiée, interceptée et traitée selon sa nature.

Pour veiller au maintien de la conformité à la réglementation et prévenir la fuite d'informations critiques, la passerelle SWG peut se connecter à des bases de données existantes et fournir des modèles standard et des dictionnaires de termes courants pouvant indiquer la présence de données sensibles dans une communication spécifique.

Selon le contenu, l'anonymisation contextuelle permet de surveiller les données sensibles et, si besoin, de les anonymiser automatiquement afin que la communication puisse se poursuivre, mais sans les informations enfreignant la politique qui sont donc supprimées. Ce processus peut s'appliquer aussi bien aux propriétés d'un document qu'à un historique des modifications pouvant contenir des données sensibles.

Inspection du contenu en profondeur

Une inspection intelligente et approfondie du contenu garantit des communications sans risques sur les réseaux sociaux. Le moteur d'inspection approfondie du contenu de Clearswift peut faire la différence entre un tweet innocent et un autre potentiellement dangereux. Une analyse contextuelle peut empêcher des utilisateurs de télécharger vers un serveur des informations et des images faisant l'objet de restrictions. L'association de politiques sensibles au contenu et au contexte réduit considérablement le nombre de faux positifs, avec moins de ressources à gérer pour administrer une stratégie efficace de prévention des fuites de données.

Sécurité Web à base de politiques

Intuitive et puissante, l'interface utilisateur simplifie les tâches d'administration, réduit les erreurs et minimise les coûts d'exploitation. La politique souple et facile à configurer de la passerelle est accompagnée de fonctionnalités complètes de reporting et d'audit.

Contrôles de politiques Web 2.0 souples

Clearswift facilite la configuration de politiques pour les sites de réseaux sociaux les plus populaires, tels que Facebook, LinkedIn, Twitter et YouTube, avec des politiques spécifiques. Cette fonctionnalité permet de configurer différentes politiques départementales, chaque route étant fournie avec des règles de contenu pré-remplies pour définir des politiques selon les ressources du site Web. En retour, les employés sont libres d'utiliser le Web social pour innover et développer l'activité de votre entreprise. Des fonctionnalités de reporting et d'audit de grande qualité fournissent de précieuses informations sur l'utilisation de l'information sur vos réseaux. Elles garantissent la protection contre les menaces entrantes, empêchent la fuite de données et maintiennent l'utilisation productive des ressources réseau de votre entreprise.

Si vous vous préoccupez des fuites de données possibles via Facebook, le webmail et autres sites similaires, vous pouvez continuer d'y autoriser l'accès mais en contrôlant le flux des données sortantes au moyen de politiques d'inspection et d'anonymisation. YouTube peut contenir du contenu inapproprié, mais vous pouvez autoriser l'accès uniquement aux vidéos autorisées. Les politiques granulaires de la solution Clearswift SECURE Web Gateway vous aident à atténuer les fuites de données, les risques légaux et réputationnels et aussi à garantir la conformité à la réglementation.

Expressions courantes prédéfinies pour les informations personnellement identifiables (IPI) et de carte de paiement (PCI)

- Numéro d'identité et d'assurance
- Numéros de carte de crédit
- Numéro de sécurité sociale
- Numéro de compte bancaire international (IBAN)

Dictionnaires de conformité éditables

- Loi GLBA (Gramm-Leach-Bliley Act), Loi HIPAA (Health Insurance Portability and Accountability Act), SEC (Securities and Equities Commission) et SOX (Sarbanes Oxley)

Règles de politiques contextuelles pour Facebook et autres sites Web 2.0

- Protection contre les menaces entrantes
- Protection contre les fuites de données
- Règles spécifiques pour Facebook

Intuitive et puissante, cette interface utilisateur simplifie les tâches d'administration, réduit les erreurs et minimise les coûts d'exploitation.

Protection contre les menaces entrantes

La solution SECURE Web Gateway s'appuie sur une licence Kaspersky et/ou Sophos qui fournit une protection actualisée de façon permanente et automatique en vérifiant si de nouvelles signatures de virus, malware et spyware ont été ajoutées à la base de données hébergée dans le Cloud. Les moteurs antivirus prennent également en charge des analyses heuristiques et comportementales.

Ces technologies sont enrichies par le moteur d'inspection approfondie du contenu qui empêche le téléchargement de scripts suspects et d'autres contenus à haut risque tels que des exécutables. Qui plus est, le contenu actif peut être détecté dans les documents et contenus HTML, avec en option une fonction de nettoyage des codes.

Il est possible de rechercher du texte dans du contenu Web et d'appliquer une politique en fonction du contexte et de la direction du flux.

- **URL:** prévention des recherches inappropriées ou autorisation une fois la hiérarchie informée
- **Documents:** prévention du téléchargement de données sensibles vers des sites Web 2.0 ou via webmail
- **Page Web:** blocage des pages contenant des insultes et susceptibles d'offenser
- **En-têtes HTTP:** blocage des anciennes versions de navigateur non corrigées

Filtrage d'URL de pointe

Actualisée chaque jour, la base de données URL de Clearswift contient 84 catégories. Elle référence des millions de sites et des milliards de pages Web. En outre, cette base de données gère une base supplémentaire qui contient des catégories dédiées au malware et au hameçonnage et qui est actualisée toutes les heures.

Catégorisation en temps réel

Cette fonctionnalité détecte quotidiennement les nouveaux sites inappropriés, les proxies distants, la pornographie et le piratage. Le moteur de catégorisation en temps réel de la passerelle SWG est entraîné à reconnaître les caractéristiques de ces sites et à y interdire l'accès.

Politique de durée et de quota de navigation

Des politiques élaborées permettent de définir à la fois le moment de la journée et la durée totale quotidienne de navigation d'un utilisateur pour des catégories de sites ou des sites spécifiques.

Options de déploiement souple

C'est vous qui décidez du mode d'achat et de déploiement de la passerelle Clearswift SECURE Web Gateway. Disponible sous la forme d'une appliance matérielle pré-installée ou d'une image logicielle qui peut être chargée sur tout un éventail de plateformes matérielles et de Clouds publics tels qu'AWS et Azure, cette solution peut également être virtualisée dans un environnement VMware.

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

clearswift
RUAG Cyber Security

Fonctionnalités	Avantages
Politique	
Contrôles de politiques souples et granulaires	Définition aisée de politiques pour faciliter et autoriser l'utilisation du Web 2.0 tout en minimisant le risque.
Politiques pour Facebook, LinkedIn, Twitter et YouTube	Accès autorisé aux sites Web 2.0, mais uniquement au contenu et aux fonctionnalités qu'autorise votre politique.
Droits d'accès au Web avec définition d'une durée et d'un quota par utilisateur	Définition de politiques de plages horaires, de durée et de quota de navigation sur des sites Web sélectionnés afin d'en limiter l'accès.
Direction à appliquer à la politique pour fournir du contenu supplémentaire	Prévention du téléchargement de certains types de fichiers (feuilles de calcul, etc.) vers un serveur mais téléchargement autorisé vers un poste de travail.
Pages d'informations acceptables	Utilisation de 'pages à contenu acceptable' pour rappeler à l'utilisateur que son utilisation du Web est surveillée et soumise aux politiques de l'entreprise.
Hygiène	
Antivirus avec recherche assistée dans le Cloud et analyses heuristiques et comportementales	Neutralisation d'infections dues à des malware connus et inconnus qui pénètrent sur ou quittent le réseau.
Analyse anti-spyware bidirectionnelle	Neutralisation des spyware, adware, key loggers et appels "spyware call home" depuis des machines infectées.
Base de données de filtrage d'URL avec 84 catégories	Accès interdit à des sites inappropriés et fourniture de contexte pour des rapports Web.
Catégories Malware, Hameçonnage et Spyware	Accès interdit aux URL et sites à haut risque connus avec mises à jour toutes les heures.
Moteur de catégorisation en temps réel	Accès interdit aux sites nouveaux ou non répertoriés hébergeant du contenu inapproprié.
Inspection contextuelle à 50 niveaux	Interception des exécutables dont ActiveX en cours de téléchargement, y compris embarqués dans d'autres types de fichiers ou des conteneurs de fichiers compressés.
Suppression des codes actifs*	Détection et suppression du contenu actif tel que les macros et les scripts à l'intérieur des documents ou du contenu HTML.
Inspection du contenu	
Identification de type fichier binaire	Identification précise à base de signature avec possibilité de définir ses propres signatures de fichiers.
Inspection et analyse HTTPS complètes	Lecture du trafic chiffré pour prévenir les malware et les fuites de données sensibles sortantes.
Analyse lexicale et règles pour les expressions courantes	Recherche de mots-clés et d'expressions dans le contenu de la communication en faisant correspondre des expressions simples ou des caractéristiques plus complexes avec des expressions courantes, des recherches booléennes et positionnelles pour identifier les caractéristiques des données sensibles. Création de jetons personnalisés permettant des profils de recherche plus sophistiqués pour réduire le nombre de faux positifs et possibilité de lancer une vérification du texte vers des sources de données structurées.
Anonymisation contextuelle	Anonymisation automatique du texte généré par des applications courantes à partir de mots-clés ou de jetons prédéfinis. Suppression des informations d'historique indésirables ou sensibles des fichiers, y compris les propriétés personnalisées voire "inattendues" (ou non conformes). Détection du contenu actif et suppression de toute trace de ce dernier.
Modèles de données sensibles prédéfinis	Identification des numéros de carte de crédit, de compte bancaire, de sécurité sociale et d'identité.
Politiques de conformité	Dictionnaires multilingues d'injures et de conformité éditables intégrant GLBA, HIPAA, SEC, SOX, PCI et IPI pour réduire au minimum les risques réputationnels et terminologiques.
Administration et Reporting	
Interface Web intuitive	Facilité d'utilisation sans aucun apprentissage nécessaire de syntaxe complexe ou de commandes Linux.
Rapports personnalisables prédéfinis	Rapports graphiques faciles à modifier, lancer et partager avec une analyse en profondeur intuitive.
Reporting programmé	Possibilité de lancer des rapports manuellement ou régulièrement et d'automatiser leur envoi par email.
Reporting consolidé multi-passerelle	Vue consolidée du reporting des activités des utilisateurs pour faciliter l'analyse et le partage des données d'administration.
Intégration Active Directory (AD) et LDAP	Contrôle complet des politiques utilisateur pour un reporting souple sur les politiques et l'audit par groupe ou individu.
Reporting programmé sur le spyware	Contrôle du spyware et identification des équipements utilisateur à remédier.
Alertes SNMP, SMTP et SYSLOG	Les alertes d'administration SNMP ou SMTP facilitent un déploiement "sans surveillance manuelle" tandis que les fichiers journaux peuvent être automatiquement consolidés via SYSLOG.
Serveur proxy avec fonctionnalité de mise en cache HTTP	Disponible sous la forme d'une appliance matérielle pré-installée ou d'une image logicielle qui peut être chargée sur tout un éventail de plateformes matérielles, cette solution peut aussi être virtualisée dans un environnement VMware.

* Option tarifée