FORTRA

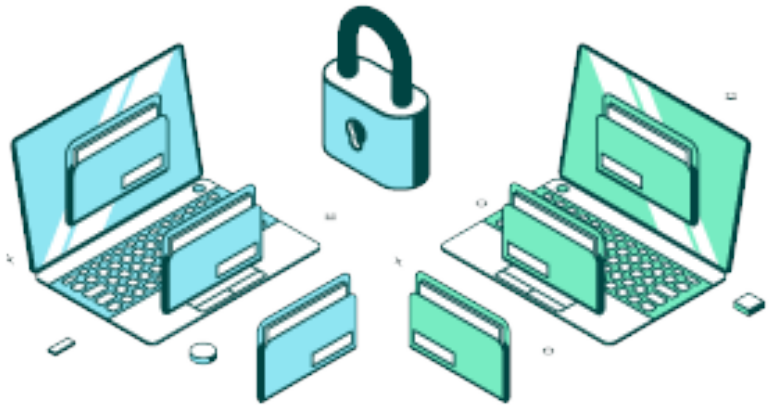
BlueFinch ESBD

GoAnywhere + Clearswift

Le partage d'informations est de plus en pus utilisé entre partenaires commerciaux a transformé la collaboration à distance des entreprises. Cependant, ce besoin de partager de l'information s'accompagne du risque d'exposer le mauvais contenu.

Il est donc primordial de savoir comment les données peuvent être partagées en toute sécurité. Les fichiers qui contiennent de confidentielles visibles dans le corps du fichier ou contenu dans les métadonnées, peuvent être partagés par erreur. De même, l'envoi et la réception de fichiers à destination de partenaires peuvent potentiellement ouvrir la porte à des logiciels malveillants ou des menaces cachées dans les transferts de fichiers s'ils ne sont pas correctement sécurisés.

La combinaison GoAnywhere MFT et Clearswift offre un partage d'informations avec un niveau de gestion et de sécurité sans précédent, garantissant que les informations transférées ne sont accessibles qu'aux parties autorisées et débarrassées de toutes menaces malveillantes.



Solution SecureCollaboration

Les entreprises doivent pouvoir avoir un contrôle total sur la façon dont les informations circulent et sont partagées, tant en interne qu'en externe. La gestion des flux de données, peut être facilement définis pour échanger des informations via un portail, transférer des fichiers par FTP sécurisé ou même déplacer des fichiers dans des partages de réseau.

En intégrant une couche supplémentaire d'inspection et d'assainissement par le biais du protocole ICAP, des contrôles peuvent être mis en place pour appliquer des politiques de sécurité et de conformité adaptatives aux fichiers transférés.

La passerelle Clearswift SECURE ICAP Gateway (SIG) est la seule solution de protection des informations critiques complètement automatisée pour contrôler totalement les informations qui circulent lors de la navigation Web de vos utilisateurs. Optimisez la sécurité de votre infrastructure Web existante à l'aide du protocole ICAP pour intégrer facilement la technologie unique de Clearswift et appliquer automatiquement la solution brevetée d'anonymisation contextuelle de Clearswift sur vos informations critiques.

BlueFinch ESBD +33 9 70 75 61 13 sales@bluefinch-esbd.com bluefinch-esbd.com

Clearswift SECURE ICAP Gateway

Prévention des fuites de données

Souvent, le déploiement d'outils de prévention des fuites de données (DLP) échoue en raison d'un manque de précision, d'une complexité et des gros coûts d'exploitation associés. Clearswift résout ces problèmes opérationnels en fournissant des fonctionnalités de pointe bidirectionnelles qui limitent le partage d'informations non autorisé, tout en réduisant le plus possible les occurrences de faux positifs qui perturbent la productivité de l'entreprise.

Grâce à une connexion aux sources de données existantes et à une analyse lexicale souple, la solution ICAP Gateway identifie avec précision les risques réels de fuites de données avant qu'elles ne se produisent. L'intégration au serveur IGS de Clearswift chargé de la gouvernance de l'information, renforce la protection de l'information non seulement en détectant
le contenu (empreintes) de fichiers totalement ou partiellement enregistrés, mais aussi en suivant chaque élémen t d'information transitant par la passerelle ICAP.

Le déploiement est grandement simplifié et intégré à votre infrastructure existante grâce à cette passerelle.
Des actions souples permettent de déclencher des workflows suite à des violations de politiques ou de modifications de contenu pour maintenir la collaboration dans le respect des réglementations.

Inspection du contenu en profondeur

Avec le moteur d'inspection approfondie de contenu de Clearswift, les entreprises peuvent désassembler complètement le flux de communication pour comprendre et protéger pleinement les informations critiques en cours d'échange. Ceci peut également s'appliquer aux applications Web 2.0 et être adapté aux besoins de chaque utilisateur, rôle et département de
l'entreprise.L'analyse contextuelle empêche les utilisateurs d'envoyer des informations à diffusion restreinte tandis que les
politiques granulaires appliquent à des utilisateurs (non) autorisés une politique différente suite à l'inspection du contenu qu'ils comptaient partager. Nombreuses sont les entreprises qui n'ont conscience du risque
d'échangesd'informations critiques non autorisés. Clearswift permet d'appliquer des politiques souples en mode surveillance pour aider à identifier et
à traiter le problème tout en optimisant ces politiques avant leur mise en application.

Anonymisation contextuelle

La passerelle Clearswift SECURE ICAP Gateway étend les attributs uniques de l'anonymisation contextuelle à l'infrastructure de sécurité Web existante de l'entreprise. Avec cette technologie sans égale, le contenu peut être modifié en temps réel lors de son analyse afin que les informations échangées soient conformes aux politiques de sécurité de l'entreprise. Les métadonnées, l'historique de révision, les propriétés d'un document et autres éléments cachés et non vérifiés tels que des exécutables peuvent être facilement supprimés pour protéger vos informations critiques.

Il est possible de détecter et de nettoyer le contenu actif embarqué sous la forme d'exécutables, de scripts ou de macros pour empêcher des menaces inconnues ou des menaces persistantes avancées (APT) d'accéder aux actifs de votre entreprise.

Associée à des règles d'analyse de l'information, l'anonymisation supprime et remplace le contenu confidentiel ou offensant qui est téléchargé vers un poste de travail ou un serveur.

BlueFinch ESBD +33 9 70 75 61 13 sales@bluefinch-esbd.com bluefinch-esbd.com

Les avantages

Collaboration sécurisée

- Les informations sont échangées en permanence. GoAnywhere fournit une solution pour échanger des informations au sein de l'organisation ou avec des tiers avec un contrôle d'accès.
- La passerelle Clearswift SECUREICAP Gateway vient compléter la capacité de GoAnywhere à contrôler les informations en appliquant une inspection approfondie du contenu, une prévention des pertes de données, une aide à la mise en conformité et l'obstruction des menaces d'infecter l'entreprise.
- La solution combinée permet de répondre aux besoins d'échanges sécurisés des informations par les utilisateurs.

Protection contre les cybermenaces

- Toute communication entrante peut constituer une menace pour une entreprise et les échanges de fichiers n'y échappent pas. Les fichiers reçus de tiers peuvent contenir une menace intégrée dans un document inoffensif.
- Les cybercriminels essaient continuellement de trouver le moyen le plus facile pour attaquer les entreprises et l'utilisation du partenaire moins bien protégé devient une voie d'attaque. Clearswift et GoAnywhere MFT proposent une solution combinée qui stoppe les menaces tout en permettant la poursuite de l'échange d'informations commerciales.
- Les malwares, et plus particulièrement les spywares et les ransomwares, sont fréquemment distribués sous forme de contenu actif caché dans des formats de documents courants, comme les fichiers Microsoft Office ou les documents PDF. La protection avancée contre les menaces de Clearswift permet de décomposer les fichiers, identifier le contenu actif et le neutraliser pour éliminer ces risques.
- Avec la flexibilité offerte par les flux de travail de GoAnywhere, vous pouvez complètement automatiser vos transferts de fichiers. En s'intégrant à Clearswift SECURE ICAP Gateway, ces processus peuvent être contrôlés afin d'identifier et de neutraliser les menaces qui pourraient facilement se propager.

Retrouvez le contrôle total des informations

- Les réglementations relatives à la confidentialité des données, telles que le RGPD, exigent que les entreprises contrôlent les informations qui leur sont communiquées. GoAnywhere MFT associé à la passerelle SECURE ICAP de Clearswift fournissent un moyen d'identifier les utilisateurs accédant ou partageant des informations et d'appliquer la politique appropriée. En automatisant la détection et le nettoyage des informations soumises à des réglementations, les entreprises sonten mesure de faire face à la quantité croissante d'informations échangées tout en gardant le contrôle des informations et en permettant lescommunications commerciales.
- Les documents sont généralement révisés par différents membres de l'équipe avant d'être publiés. Mais l'historique des modifications ainsi que les commentaires et propriétés sont stockés sous forme de métadonnées dans les fichiers. Ces informations cachées sont également soumises aux conformités réglementaires, en plus de présenter un risque élevé de perte de données. GoAnywhere MFT de HelpSystems utilise la passerelle Clearswift SECURE ICAP Gateway pour inspecter, détecter et nettoyer les métadonnées et l'historique des révisions des fichiers transférés.

GoAnywhere + Clearswift

Partagez des informations sensibles internes et externes à votre entreprise en toute sécurité. Clearswift et HelpSystems présentent la première solution à intégrer une protection contre les menaces avancées et une prévention adaptative des pertes de données p our les transferts de fichiers gérés (MFT).

La rédaction et l'assainissement des données garantissent que les informations partagées ne sont accessibles qu'aux parties autorisées et à l'abri des codes malveillants.

About GoAnywhereMFT

GoAnywhere MFT est une solution de transferts de fichiers primée par Info-Tech Research Group qui rationalise, sécurise et automatise les transferts de fichiers critiques.

La solution centralisée permet de vous connecter aux systèmes internes et externes à l'entreprise et d'échanger des données chiffrées à l'aide de protocoles standards comme OpenPGP, AES, FTPS, SFTP, HTTPS, AS2 et GPG.

BlueFinch ESBD +33 9 70 75 61 13 sales@bluefinch-esbd.com bluefinch-esbd.com