

ARgon

Adaptive Redaction for Email
Powered by Clearswift

ARgon utilise la technologie unique d'anonymisation contextuelle développée par Clearswift et résout les problèmes des solutions traditionnelles de prévention des fuites de données (DLP) en supprimant automatiquement et uniquement le contenu qui enfreint la politique de sécurité, sans interférer sur la transmission du reste du courrier électronique et des pièces jointes. Cette approche assure une collaboration continue tout en garantissant la protection de l'information sensible.

L'efficacité de la DLP est déterminée par la précision et le flux de travail de la solution. Trop de solutions DLP sont achetées mais jamais déployées car trop difficiles à configurer ou parce qu'elles génèrent trop de faux positifs, ce qui augmente le coût d'exploitation et diminue la productivité en raison d'une communication perturbée.

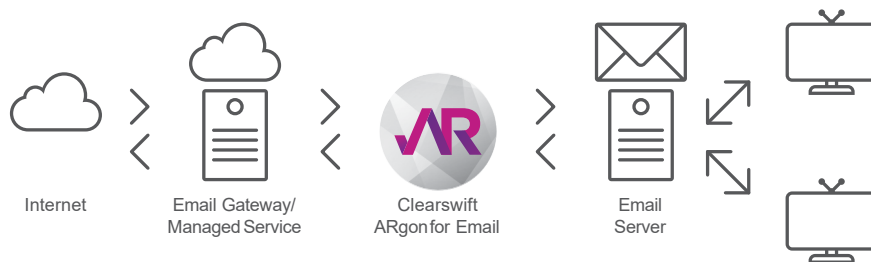
ARgon s'utilise dans des environnements sans solution de DLP ou pour en améliorer l'existante. Dans les deux cas, ARgon supprime des courriers entrants et sortants, les toutes dernières formes de menace pour l'information. Dans les environnements dotés d'une solution DLP, ARgon réduit les faux positifs en supprimant automatiquement le contenu susceptible de provoquer l'arrêt et le blocage de la communication.

La solution ARgon for Email offre trois fonctionnalités clés de l'anonymisation contextuelle qui sont:

- Anonymisation des données : Supprime de l'email et de ses pièces jointes le contenu visible qui enfreint la politique de sécurité.
- Suppression des métadonnées : Supprime les méta données, l'historique de révision, etc.
- Suppression des codes actifs : Supprime le contenu actif embarqué dans les documents reçus.

Déploiement

ARgon est déployé entre le service d'hygiène du courrier électronique (et/ou DLP) et le serveur de messagerie interne.



- ARgon for Email utilise la technologie de messagerie SMTP standard pour garantir la compatibilité avec d'autres solutions de passerelle de messagerie
- Le service de passerelle de messagerie peut être celui d'un quelconque fournisseur et être déployé sur site ou hébergé.
- Le serveur de messagerie peut être Exchange, Lotus Notes, Domino ou Groupwise.
- Les tests pour justifier la valeur de la solution (PoV – Proof of Value) peuvent s'appuyer sur des déploiements "Side Car" ou "En série"

Quarantaine

Le cloisonnement entre les services d'hygiène et d'inspection/remédiation du contenu d'ARgon permet de transmettre les événements liés aux violations de politiques aux destinataires suivants:

- L'équipe Informatique qui se concentrera sur les virus et les malware dangereux;
- Les responsables de l'entreprise et l'équipe chargée des audits qui se concentreront sur les violations relatives au contenu sensible.

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

Politiques

Argon for Email est fourni avec des politiques par défaut pour réduire immédiatement les risques dès son installation. Ces politiques ou règles de sécurité par défaut peuvent ensuite être renforcées si des niveaux de granularité ou de conformité plus élevés s'avèrent nécessaires.

Fonctionnalités d'anonymisation contextuelle	Politique standard
Anonymisation des données	Supprime les informations personnellement identifiables et de carte de crédit dans tous les emails et document sortants
Suppression des métadonnées	Supprime toutes les propriétés des documents, l'historique de révision et les informations de sauvegarde rapide
Suppression des codes actifs	Supprime tout le contenu actif des documents entrants et sortants

Autorisation de diffuser

Lorsque la fonctionnalité d'anonymisation contextuelle a supprimé certaines informations pour empêcher la violation des politiques, mais que le reste de l'information doit être diffusé, il suffit au responsable hiérarchique de l'expéditeur (administrateur autorisé, délégué à la protection des données, etc.) de cliquer sur le lien communiqué dans l'email qu'il a reçu. Pour ce faire, il suffit d'intégrer la solution à Microsoft Active Directory ou à un service LDAP pour qu'elle puisse découvrir les relations hiérarchiques au sein de l'entreprise.

Reporting

Un certain nombre de rapports standard sont fournis avec la solution ARgon pour indiquer le nombre d'emails et de pièces jointes auxquels la politique a été appliquée. Ces rapports peuvent également être utilisés en mode Surveillance, c'est-à-dire lorsqu'aucune action n'est entreprise, afin d'afficher le nombre de communications concernées. Cela s'effectue généralement lorsque le système est à l'essai ou déployé pour la première fois dans le cadre de la formation du personnel.

Fonctionnalités	Avantages
Solution fournie sous forme de logiciel ou d'appliance virtuelle ou physique	Déploiement du logiciel et de l'appliance en quelques minutes. Solution qui ne nécessite pas des semaines à son implémentation et avec des services potentiellement intrusifs.
Service d'hygiène agnostique	S'appuyant sur le protocole SMTP, ARgon fonctionne de manière transparente avec les produits Cisco, McAfee, Symantec, Sophos, Microsoft et bien d'autres encore.
Assistant d'installation simple en 5 étapes – installation et configuration de politiques par défaut en quelques minutes seulement.	Simplicité d'achat, de déploiement et de support pour un coût total de possession minimal. Protection de l'IP de l'entreprise et conformité rapide à la législation.
Indépendance vis-à-vis des serveurs de messagerie - Support d'Exchange, GroupWise, Lotus Notes, SMTP et POP	Perturbation minimale de l'environnement d'exploitation en place et possibilité de choisir la solution de sécurité de messagerie la mieux adaptée aux besoins évolutifs de l'entreprise
Inspection du contenu en profondeur	Recherche de contenu délibérément caché ou diffusé par inadvertance ou par erreur. Inspection de la construction des documents complexes, par exemple un objet imbriqué dans une feuille de style Excel elle-même embarquée dans un document Word.
Haute performance	Traitement de plusieurs milliers de messages par heure sur des serveurs standard ou vSphere pour réduire les dépenses d'investissement
Suppression des violations	Conformité aux réglementations externes et internes tout en maintenant l'activité ou la productivité de l'entreprise
Gestion interne	Violations de sécurité traitées plus rapidement en fournissant du contexte aux responsables hiérarchiques pour qu'ils statuent sur le déblocage et l'envoi d'un message en toute sécurité

Principales caractéristiques techniques	Avantages
Chiffrement	Utilisation du protocole SMTP standard et support du chiffrement TLS
Anonymisation du texte	Anonymisation du texte dans le corps du message électronique (texte et HTML) ainsi que dans les fichiers MS Office Word, Excel et PowerPoint 2007+, Open Office Writer, Calc et Impress et PDF
Suppression des métadonnées	Suppression des métadonnées dans les fichiers MS Office Word, Excel et PowerPoint 2007+, Open Office Writer, Calc et Impress et PDF
Suppression des codes actifs	Suppression des codes actifs dans le corps des messages électroniques HTML ainsi que dans les fichiers MS Office Word, Excel PowerPoint 2007+, Open Office Writer, Calc et Impress et PDF