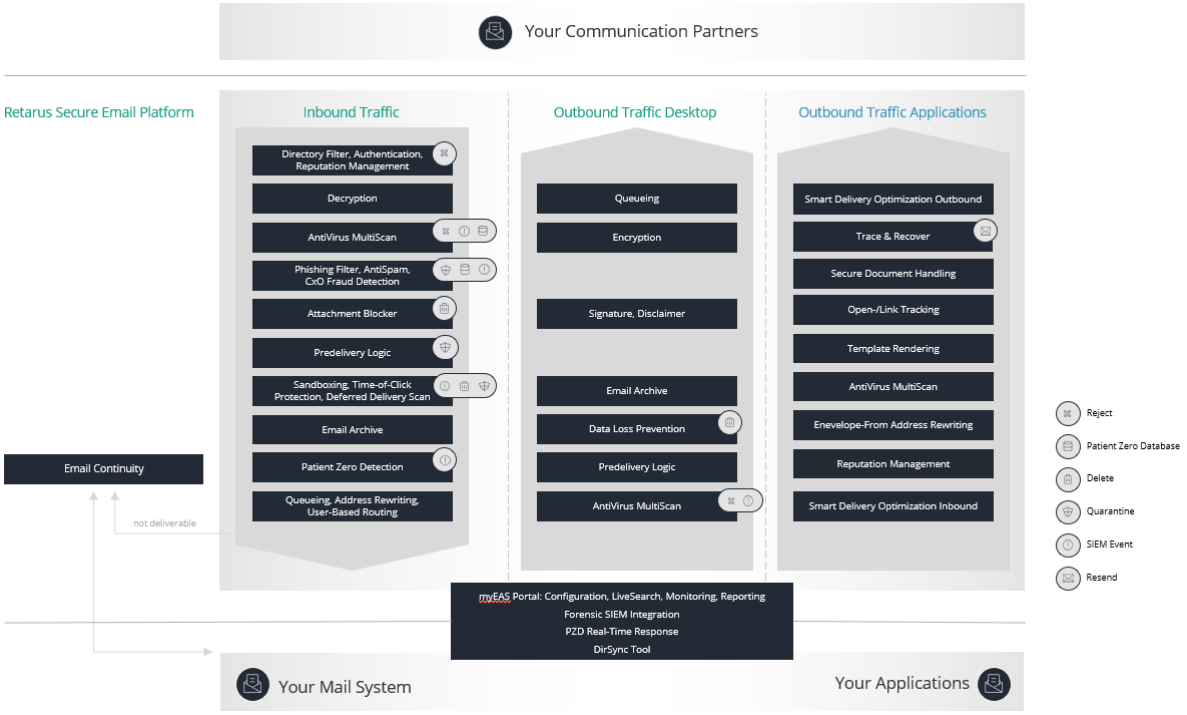
Description des services et obligations de collaboration
Retarus Secure Email Platform

La plateforme **Retarus Secure Email Platform** offre des modules pour une sécurité complète (« Advanced Threat Protection », une protection post-livraison brevetée, « Sandboxing »), un routage optimisé des emails via la « Predelivery Logic », l'archivage et le cryptage des emails et la continuité des emails. En outre, les applications commerciales existantes peuvent être connectées à la plate-forme via le module Retarus Transactional Email.

La gamme de services est structurée comme suit : **Email Cloud Gateway, Email Security, Email Compliance et Email Infrastructure.**

Sommaire

Architecture du système Secure Email Platform



Email Cloud Gateway

La passerelle Retarus Email Cloud Gateway offre des fonctionnalités de base pour gérer et sécuriser le trafic des messages SMTP. Elle peut être utilisée comme un service autonome, mais peut également être étendue en utilisant par des modules supplémentaires.

L'Email Cloud Gateway comprend les fonctionnalités suivantes :

Directory Filter / Réputation Management

Conformément aux RFC (méthode Reject), le filtre d'adresses rejette les e-mails envoyés à des destinataires non enregistrés sur le portail Enterprise Administration Services (portail EAS) de Retarus. La configuration et l'actualisation sont réalisées soit manuellement par le client via le portail EAS, soit automatiquement à travers la synchronisation des adresses, dans un format prédéfini par Retarus comprenant les carnets d'adresses et les répertoires du client.

La réputation des expéditeurs des e-mails entrants est vérifiée via la gestion de la réputation du domaine expéditeur qui complète le filtre d'annuaire. L'autorisation d'un expéditeur est validée via les mécanismes SPF (Sender Policy Framework) et DKIM (DomainKeys Identified Mail). En cas d'échec de la validation, ces e-mails sont traités conformément à la configuration du Client dans le portail EAS ou - s'ils sont activés par le Client - traités ultérieurement conformément à la spécification de la politique DMARC (Domain-based Message Authentication, Reporting & Conformance) du propriétaire du domaine (expéditeur) (actions : Aucune, Quarantaine, Rejeter).

Remarque : L'utilisation de DMARC nécessite un routage vers un enregistrement MX dédié de Retarus.

AntiVirus Multiscan 2x

Retarus numérise les messages entrants et, s'ils sont autorisés, les messages sortants pour vérifier s'il existe des virus. Pour réaliser ces analyses, Retarus utilise deux analyseurs de virus de différents fournisseurs de leur choix. Dès qu'il y a des actualisations ou de nouvelles versions de ces fournisseurs, Retarus les utilisera immédiatement pour les analyses de virus. Si un virus est détecté, Retarus supprime tous les e-mails infectés. Les destinataires respectifs des e-mails infectés, et/ou leurs administrateurs sauvegardés dans ce cas, seront informés par la gestion des quarantaines.

Protection DHA

Protection contre les attaques de type *Directory Harvest Attack* (DHA) pour le(s) domaine(s) de messagerie sélectionné(s) par le propriétaire du domaine. Les messages destinés à des destinataires non valides au sein du domaine concerné seront rejetés. La réception de messages supplémentaires pour des destinataires non valides sera limitée par le ralentissement des emails provenant de l'expéditeur identifié de ces messages.

Backscatter Protection

Protection contre la mauvaise utilisation des messages bounce générés automatiquement pour l'envoi (Backscatter).

Le backscatter est l'utilisation non autorisée de l'adresse électronique valide d'une autre personne pour des campagnes de spam. Il se peut que le serveur de messagerie des destinataires reçoive un nombre important de notifications d'état de livraison (par exemple si l'adresse de réception n'existe pas) sur l'adresse de messagerie valide de la personne qui a été utilisée comme expéditeur à son insu. Les courriers électroniques ne sont pas remis à l'expéditeur réel.

Grâce à Backscatter Protection, un nombre accru de ces messages générés automatiquement seront identifiés et filtrés, et leur remise sera empêchée grâce à l'isolement du destinataire concerné en quarantaine personnelle. Dans la quarantaine personnelle, ces messages seront marqués comme Spam NDR.

Email Backup / Queuing

Si les messages destinés au client ne peuvent pas être délivrés, Retarus stockera les messages entrants respectifs pendant 96 heures au maximum. Si l'impossibilité de délivrer ne peut pas être résolue, l'expéditeur du message recevra une notification par e-mail de cette impossibilité. Retarus essaiera de délivrer les messages à des intervalles courts réguliers lors de cette analyse de 96 heures. Si l'impossibilité de délivrer se résout pendant la durée de cette analyse, les messages entrants seront expédiés par lots par Retarus.

Large Email Handling

Le client peut définir des limitations de taille pour les e-mails entrants volumineux afin d'empêcher leur envoi direct aux boîtes de messagerie du client à partir d'une taille déterminée et de les rendre disponibles au téléchargement via Retarus. Lorsque cette fonction est configurée, le destinataire est informé de la réception d'un tel message. Le téléchargement est effectué via un lien http bénéficiant d'une authentification utilisateur simplifiée (OneClick token login).

User based Routing

Le routage basé sur les utilisateurs permet à Retarus de distribuer certains e-mails vers un serveur spécifique en fonction de leur destinataire. Ces destinataires sont définis par le client et appartiennent à un domaine donné.

Email Signature / Disclaimer

Le client peut créer des signatures ou des avis de non-responsabilité sur le portail Enterprise Administration Services Portal (portail EAS). Retarus joint aux e-mails sortants du client les signatures ou avis de non-responsabilité créés via le portail EAS. En cas d'utilisation de texte de substitution, celui-ci est extrait à partir de données issues de la synchronisation des adresses.

Email Live Search

Email Live Search permet d'effectuer un suivi en temps réel des messages sortants et entrants. Il est ainsi possible de déterminer les e-mails infectés et le virus utilisé, ainsi que les filtres et règles supplémentaires utilisés.

Access Management

Le portail Retarus Enterprise Administration (EAS-Portal) permet d'accorder des droits d'accès à des administrateurs individuels conformément aux exigences des clients, par exemple en définissant des droits d'accès différents pour certains pays, filiales, domaines ou départements.

Email Security

Retarus Email Security protège les infrastructures de messagerie complexes contre les logiciels malveillants tels que les virus, les spams, les e-mails de phishing, les ransomwares et autres menaces numériques. Les méthodes de filtrage à plusieurs niveaux et les sources de données sont constamment mises à jour et optimisées. Le traitement des données a lieu dans les propres centres de données de Retarus, conformément aux règles de protection des données actuellement en vigueur.

AntiVirus MultiScan 2x

Retarus numérise les messages entrants et, s'ils sont autorisés, les messages sortants pour vérifier s'il existe des virus. Pour réaliser ces analyses, Retarus utilise deux analyseurs de virus de différents fournisseurs de leur choix. Dès qu'il y a des actualisations ou de nouvelles versions de ces fournisseurs, Retarus les utilisera immédiatement pour les analyses de virus. Si un virus est détecté, Retarus supprime tous les e-mails infectés. Les destinataires respectifs des e-mails infectés, et/ou leurs administrateurs sauvegardés dans ce cas, seront informés par la gestion des quarantaines.

AntiVirus MultiScan 4x

Fonctionne selon le même principe qu'AntiVirus MultiScan 2x, à la seule différence que le contrôle des attaques virales est réalisé à l'aide de quatre scanners antivirus provenant de fournisseurs différents.

External Sender Visibility Enhancement

External Sender Visibility Enhancement signale les messages entrants qui utilisent un domaine d'expéditeurs attribué au client dans le champ expéditeur. Pour valider l'expéditeur, le champ d'entête MIME-FROM est utilisé. Les messages entrants sont marqués d'une icône Unicode (symbole) prédéfinie au sein de l'infrastructure Retarus avant d'être transmis à l'infrastructure du client. Le marquage a lieu dans le champ de l'expéditeur du « friendly name ».

Antispam Management and Phishing Filter (inbound)

Les messages destinés aux clients reçus par Retarus sont examinés par les différents filtres anti-spam utilisés par Retarus. Ces messages se voient ensuite affecter une probabilité de SPAM, avant d'être identifiés comme « spam potentiel » en fonction des valeurs seuil définies par le client. Les messages identifiés comme « spam potentiel » ne sont pas immédiatement distribués et sont traités conformément à la configuration définie dans Quarantaine Management. À la demande du client, les messages identifiés comme SPAM peuvent également être marqués à l'aide d'une mention spéciale avant d'être distribués (« tag and deliver »). Retarus s'appuie pour ce faire sur différentes méthodes et technologies de filtre, de modèles et d'identification. Le filtre anti-hameçonnage compare les liens contenus dans les e-mails entrants avec des référentiels spécialisés dans les URL de hameçonnage. La prise de connaissance et le traitement des messages mis en quarantaine ou marqués incombent au client et aux utilisateurs qu'il a désignés.

AntiSpam Management and Phishing Filter (outbound)

Semblable à l'AntiSpam Management and Phishing Filter (Entrant) de Retarus, l'équivalent sortant emploie la technologie reconnue de filtres antispam utilisée par Retarus. Un score de probabilité de SPAM est attribué à chaque e-mail sortant, et ceux dépassant un seuil paramétrable (établi par défaut à 60 %) sont soumis à différentes options de disposition en fonction de la configuration de vos préférences. Les options disponibles incluent le refus, la défaillance temporelle (tempfail) ou le rejet par silence, vous permettant de personnaliser la réponse afin qu'elle s'aligne à vos politiques de sécurité spécifiques. La flexibilité de la configuration s'étend à tous les niveaux de hiérarchie, vous permettant de perfectionner les paramètres au niveau du client, du domaine, du profil et de l'utilisateur. Pour activer la fonctionnalité, veuillez contacter l'équipe de Support de Retarus.

Attachment Blocker

La distribution de certaines pièces jointes d'e-mail peut être bloquée en fonction de la configuration définie par le client. Les pièces jointes peuvent être bloquées en fonction des extensions de fichier (par exemple, exe, mp3, zip) ou des types MIME utilisés. Soit le fichier joint d'un e-mail entrant est supprimé – et seul le corps de message est transmis au destinataire –, soit une copie de l'e-mail original incluant la pièce jointe est envoyée à une boîte de messagerie prédéfinie (par exemple, l'administrateur). Les destinataires peuvent être informés des pièces jointes supprimées à l'aide de notifications configurables.

Outbound Recipient Restriction

Par défaut, les e-mails sortants traités par Retarus peuvent avoir jusqu'à 600 adresses de destination. Si un e-mail dépasse ce seuil, Retarus le rejette pour les destinataires en trop. La notification dépend de la configuration de votre serveur de messagerie. Notre fonctionnalité de Restriction de destinataires sortants vous offre la possibilité d'établir un nombre maximal personnalisé de destinataires (0-600) pour les e-mails sortants. Le fait de dépasser la limite configurée peut déclencher le refus, la défaillance temporaire ou le rejet par silence, en fonction de vos préférences. Cette capacité vise à limiter les destinataires, à empêcher les divulgations d'identité et à faciliter une administration efficace. La fonctionnalité peut être configurée à tous les niveaux de hiérarchie (client, domaine, profil, utilisateur). Pour activer cette fonctionnalité, une assistance de la part de l'équipe de Support de Retarus est nécessaire au début.

Outbound Size Restriction

Par défaut, les e-mails sortants traités par Retarus peuvent avoir une taille de jusqu'à 250 Mo (256 000 Ko). La fonctionnalité de « Restriction de taille sortante » vous permet de restreindre encore davantage la taille des e-mails sortants, si nécessaire. Le fait de dépasser la limite configurée peut déclencher le refus, la défaillance temporaire ou le rejet par silence, en fonction de vos préférences. La fonctionnalité peut être configurée à tous les niveaux de hiérarchie (client, domaine, profil, utilisateur). Pour activer cette fonctionnalité, une assistance de la part de l'équipe de Support de Retarus est nécessaire au début.

Deferred Delivery Scan

Le scanner Deferred Delivery Scan (DDS) permet de soumettre des fichiers joints spécifiques à une analyse approfondie à l'aide de processus d'analyse supplémentaires. Ces analyses supplémentaires reposent sur des signatures plus actuelles. Il est ainsi possible d'éviter avec une plus forte probabilité de distribuer des contenus malveillants qui seraient passés à travers les mailles du filet lors du premier processus de scan. Dès qu'une attaque virale est constatée, Retarus supprime les messages correspondants et envoie des notifications conformément à la configuration définie dans Quarantaine Management. Dans la mesure où l'utilisation de DDS entraîne un retard de la distribution des e-mails entrants, les dispositions des accords de niveau de service relatives aux délais de distribution ne s'appliquent pas dans ce cas de figure.

Time-of-Click Protection

Les liens contenus dans les e-mails sont automatiquement réécrits (URL Rewriting). Dès que des destinataires cliquent sur les liens correspondants, ceux-ci sont contrôlés afin de détecter des adresses cibles potentiellement liées à des attaques de hameçonnage. Lorsque la page cible n'est pas identifiée comme étant une page d'hameçonnage, une redirection est immédiatement effectuée. Lorsque la page cible est bien une page d'hameçonnage, un message d'avertissement s'affiche. Après leur désactivation par le service, ces liens ne peuvent en aucun cas être directement utilisés.

CxO Fraud Detection

CxO Fraud Detection utilise des algorithmes capables d'identifier le « From-Spoofing » et le « Domain-Spoofing » afin de reconnaître les adresses d'expéditeur usurpées (appartenant par exemple à des dirigeants de haut rang). Les messages de CxO Fraud identifiés sont alors traités conformément à la configuration définie dans Quarantaine Management.

Sandboxing

Le Sandboxing permet de soumettre des fichiers joints spécifiques à une analyse approfondie. Les pièces jointes susceptibles de contenir des éléments malveillants sont exécutées sur une machine virtuelle. Leur comportement est alors contrôlé et elles sont supprimées en cas de détection d'attaque virale. Retarus utilise pour ce contrôle les solutions Sandbox provenant d'un fournisseur tiers spécialisé. En cas de détection de contenus malveillants, les messages correspondants sont traités conformément à la configuration définie dans Quarantaine Management. Dans la mesure où le Sandboxing est susceptible d'entraîner un retard de la distribution des e-mails entrants en fonction de la taille du fichier, du type de fichier et du nombre de pièces jointes, les dispositions des accords de niveau de service relatives aux délais de distribution ne s'appliquent pas dans ce cas de figure.

Patient Zero Detection®

Patient Zero Detection® crée une empreinte digitale (« Hash ») de toutes les pièces jointes lors de la réception des e-mails adressés aux destinataires du client. En cas de détection ultérieure d'un contenu malveillant dans une pièce jointe ou un lien similaire à l'aide des scanners antivirus utilisés par Retarus, il sera également possible d'identifier rapidement les destinataires de messages potentiellement malveillants déjà distribués. Dans un tel cas de figure, les administrateurs du client et, selon la configuration choisie, les destinataires de ces messages eux-mêmes, seront immédiatement informés. Le client est alors en mesure de prendre les mesures permettant d'éradiquer le code malveillant de son infrastructure ou d'empêcher sa propagation.

Patient Zero Detection® Real-Time Response

Avec Patient Zero Detection® Real-Time Response, Retarus fournit au client un logiciel qu'il peut exploiter au sein de son infrastructure. Le logiciel traite de manière automatisée les messages identifiés comme défectueux par Patient Zero Detection® dans la boîte de réception du destinataire. Ces messages peuvent ensuite être supprimés automatiquement de la boîte de réception. Pour pouvoir exploiter Patient Zero Detection® Real Time Response, le client doit utiliser « Retarus Forensic SIEM Integration » et disposer d'une connexion à Microsoft Exchange. Patient Zero Detection® Real-Time Response est soumis à des conditions d'utilisation distinctes, que le client doit observer et respecter lors de l'installation ou de l'utilisation du logiciel. Ces conditions d'utilisation sont accessibles sur le portail EAS.

Quarantaine Management

La gestion de la quarantaine permet au client ou – s'il le souhaite – à ses utilisateurs individuels, de configurer la distribution d'un rapport E-Mail-Security (résumé) à des moments déterminés. Selon les options choisies, le résumé contient une vue d'ensemble combinée des e-mails mis en quarantaine ou supprimés au cours de la période configurée en raison de la détection de graymail (par exemple, des newsletters), de virus, de spam, de hameçonnage, de sandboxing, de CxO Fraud etc. Les messages mis en quarantaine peuvent être consultés côté client par simple clic sur l'entrée correspondante du résumé au cours de la période définie (maximum 30 jours). Selon la configuration définie par le client, les destinataires individuels peuvent accéder à leur dossier de quarantaine et configurer les paramètres correspondants. Les administrateurs du client peuvent configurer les paramètres de quarantaine à l'échelle du système via le portail Enterprise Administration Services (portail EAS).

Forensic SIEM Integration

Dans le cadre de Forensic SIEM Integration, Retarus met à disposition une interface permettant au client d'accéder à des informations sur les événements et résultats (Event ou Log) issus de la vérification des messages entrants et sortants au sein de Retarus Email Security. Ce dernier peut être intégré dans un outil SIEM existant en tant que source de données supplémentaire. Les événements mis à disposition du client dépendent des options commandées et sont disponibles pour :

- AntiVirus MultiScan (Inbound et Outbound)
- Sandboxing
- CxO Fraud Detection
- Patient Zero Detection®
- Généralement, e-mails Outbound
- Généralement, e-mails Inbound

Email Compliance

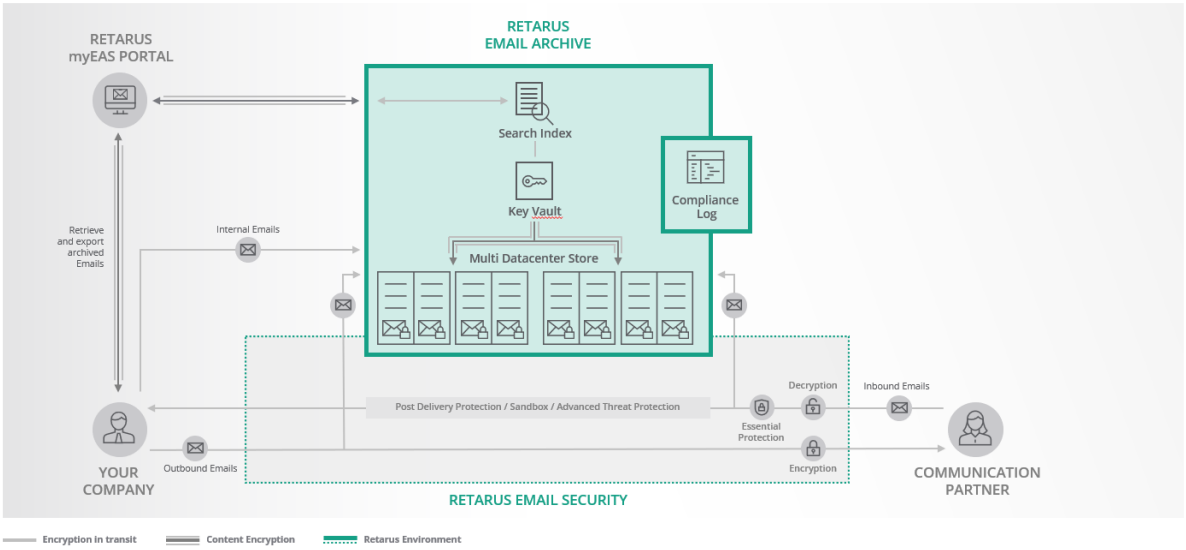
Retarus Email Archive

Retarus Email Archive stocke les communications d'e-mails entrants et sortants, automatiquement, faiblement et à long terme. Si nécessaire, les communications des e-mails internes peuvent également être stockées dans Retarus Email Archive.

Les messages transmis à Retarus Email Archive ne sont pas modifiables et ils sont récupérables et protégés contre les accès non autorisés. Ces messages sont stockés pendant la durée de l'accord, pour un maximum de dix ans, et seront supprimés à la fin de la durée convenue en conformité avec la loi, sauf convention contraire. Durant la période d'archivage, les e-mails archivés peuvent être facilement localisés et délivrés de nouveau par le client, à l'aide de plusieurs options de filtrage. Si le client souhaite exporter l'archive entière avant la fin de la période d'archivage convenue et la suppression des e-mails, il doit le demander avant la fin de la période.

L'accès de l'administrateur à l'archive des e-mails se base sur le principe de double contrôle. Les e-mails et les pièces jointes archivés peuvent être localisés rapidement grâce à de puissantes fonctionnalités de recherche, lesquelles peuvent être restreintes de façon granulaire, si nécessaire, par exemple dans le cas d'exigences en matière de protection des données.

Un protocole d'accès complet sera créé automatiquement.



Fonctionnalités :

- Stockage fiable à long terme de tous les e-mails entrants et sortants
- Stockage des données non modifiables sécurisé basé sur un cryptage hybride
- Informations de suivi fournies via EAS Live Search
- Protocole d'accès créé automatiquement
- Support pour le respect des exigences réglementaires
- Messages récupérables, y compris les pièces jointes
- Accès basé sur le principe de double contrôle via le portail administratif Internet de Retarus
- Fonctionnalité de recherche puissante avec option de configuration pour la conformité en matière de protection des données : localisation d'e-mails en fonction de l'expéditeur, du destinataire ou du format du fichier joint ; stockage paramétrable des (méta) données respectives pour rechercher par objet, texte entier ou nom de la pièce jointe.

Options à la demande

- Archivage des communications d'e-mails internes via la journalisation (Microsoft Exchange ou M365 Exchange Online)
- Accès sécurisé et pratique pour les administrateurs du client via l'authentification unique
- Importation d'e-mails depuis d'autres systèmes d'archivage (idéalement sous format EML)
- Exportation d'e-mails archivés vers des stockages de données externes
- Utilisation des clés (publiques) propres au client (le client conserve les clés privées)

Retarus Email Encryption

Retarus Email Encryption contribue à garantir l'intégrité, l'authenticité et la confidentialité des e-mails des clients. Pour ce faire, avant d'être envoyés au destinataire, les e-mails et leurs pièces jointes sont chiffrés et/ou signés dans le système Retarus : cela peut être effectué soit automatiquement selon des règles et règlements prédéfinis, soit par l'utilisateur. Un contrôle antivirus commissionné est effectué pour les messages sortants avant le chiffrement et pour les messages entrants après le déchiffrement.

Fonctionnalités supplémentaires :

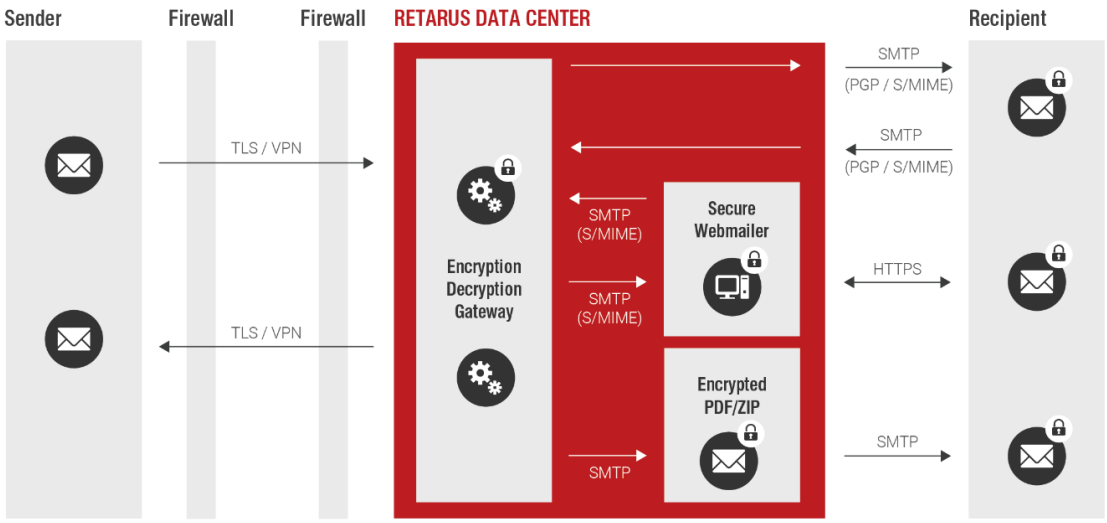
- Adoption d'infrastructures à clés publiques (PKI) existantes
- Utilisation additionnelle de certificats S/MIME existants et valables
- Support des normes Open PGP, PGP et S/MIME
- Intégration des politiques de cryptage propres au client
- Mise à disposition des compléments de Microsoft Outlook pour contrôler les actions de cryptage et/ou la signature de messages
- Mise à disposition de moyens de communication cryptée alternatifs via Retarus Secure WebMailer ou via l'envoi de fichiers PDF ou ZIP cryptés
- Intégration facultative d'un Trust Center officiel (actuellement SwissSign) pour la création de certificats S/MIME conformément à la norme X.509
- Synchronisation utilisateur automatisée pour la création et le renouvellement de certificats (à la demande)

User Synchronization for Encryption (USE

La Synchronisation utilisateur pour cryptage (USE) est une solution qui simplifie la gestion des utilisateurs du cryptage, des groupes et de leurs S/MIME ou clés PGP associés. Avec pour objectif d'améliorer l'expérience utilisateur et de réduire l'intervention manuelle, l'USE automatise le processus de renouvellement, de vérification et de révocation des certificats et des clés en contrôlant les dates d'expiration et en mettant en marche la mesure nécessaire.

- Capable d'importer en toute sécurité des utilisateurs de cryptage et de les assigner à des groupes prédéfinis.
- Gère les politiques en fonction des exigences du client et des groupes d'utilisateurs.
- Automatise la création/révocation et synchronisation de S/MIME (SwissSign).
- Effectue la distinction entre certificats personnels et certificats d'équipe pour éviter les perturbations.
- Propose un renouvellement de certifications entièrement ou semi-automatisé.
- Crée/supprime des clés PGP et synchronise les clés privées correspondantes pour chaque utilisateur.
- Permet l'importation de clés/certificats créés/achetés séparément par les clients.
- Régit une notation pour l'administration des politiques de cryptage spécifiques au client de façon lisible.
- Capable de générer des rapports de synchronisation et des rapports transactionnels de S/MIME pour la conformité et la vérification.
- Les rapports peuvent être reçus par e-mail ou stockés sur le partage SFTP pour leur recueil.

Architecture du système Retarus Email Encryption



Digital Signature / Certificates

Retarus Email Encryption permet de signer les e-mails sortants avec des clés PGP ou des certificats S/MIME, de manière manuelle ou automatisée selon un ensemble de règles. Dans le cas de messages entrants, l'utilisateur peut facilement reconnaître le résultat de la vérification de la signature grâce à des informations transparentes. En plus des certificats S/MIME selon la norme X.509 (certifications d'e-mail de classe 2), les certificats S/MIME d'un Trust Center (actuellement SwissSign) peuvent être utilisés. Ces derniers sont mis à disposition via l'infrastructure à clé publique gérée (Managed public key infrastructure ou MPKI). La condition préalable est qu'en plus des conditions de Retarus, d'autres conditions du Trust Center soient acceptées.

Secure WebMailer

Secure WebMailer est un portail Web sécurisé permettant aux clients d'échanger des e-mails chiffrés avec des destinataires qui n'utilisent aucune passerelle S/MIME ou PGP. Un lien peut être utilisé pour accéder à une boîte de réception individuelle / personnelle qui a été automatiquement créée à cet effet dans Retarus Secure WebMailer. Toutes les connexions sont chiffrées par le protocole HTTPS. Le mode de transmission (par e-mail ou SMS*) des données personnelles d'accès à l'expéditeur et au destinataire respectifs des notifications par e-mail ainsi qu'une conception optionnelle propre à l'entreprise du Secure WebMailer sont définis avec le client dans le cadre de l'atelier initial Email Encryption Workshop.

Encrypted PDF /ZIP

Retarus offre la possibilité de transmettre des informations confidentielles sous la forme d'un document PDF ou d'un fichier ZIP, tous deux sécurisés par un mot de passe. Le texte de l'e-mail ainsi que toutes les pièces-jointes sont intégrés dans un fichier PDF ou ZIP transmis au destinataire de manière chiffrée. La transmission du mot de passe pour ouvrir le document PDF ou le fichier ZIP, ainsi qu'une adaptation optionnelle du modèle utilisé sont définies avec le client dans le cadre de l'atelier initial Email Encryption Workshop.

Initial Email Encryption workshop

Email Encryption Workshop est une étape requise pour la configuration du service Retarus Email Encryption. Lors de cet atelier, le client définit avec Retarus ses critères spécifiques nécessaires pour l'installation du service. L'atelier comprend, entre autres :

- Introduction à la cryptographie
- Présentation des standards établis
- Examen de l'infrastructure actuelle
- Analyse des exigences spécifiques au client et des directives de sécurité
- Définition des flux de travail et des processus, par ex. en ce qui concerne le chiffrement / la signature ou la collecte des clés publiques
- Définition de la mise en page et du contenu des notifications par e-mail
- Définition pour l'utilisation du Secure WebMailer (par ex. transmission de données d'accès)
- Définition pour l'utilisation d'un document PDF chiffré (par ex. transmission du mot de passe)

Selon les résultats, le mandant de chiffrement spécifique au client est ensuite installé dans le système Retarus sur la base des standards S/MIME et PGP ou de méthodes de chiffrement alternatives (Secure WebMailer / PDF ou ZIP chiffré).

Extension for machine- and/or application-generated messages (eBusiness user)

Le traitement des messages générés par des machines et/ou des applications à partir d'automatismes fixes, d'applications de portail ou de solutions liées à un processus (comme par ex. un module de signature) s'effectue via une licence dite eBusiness. Chaque adresse d'expéditeur d'une telle application se voit attribuer une licence d'utilisation eBusiness distincte. Avec l'utilisation optionnelle des certificats S/MIME, Retarus gère pour le compte du client les certificats de classe 2 de la catégorie « Argent ».

Data Loss Prevention

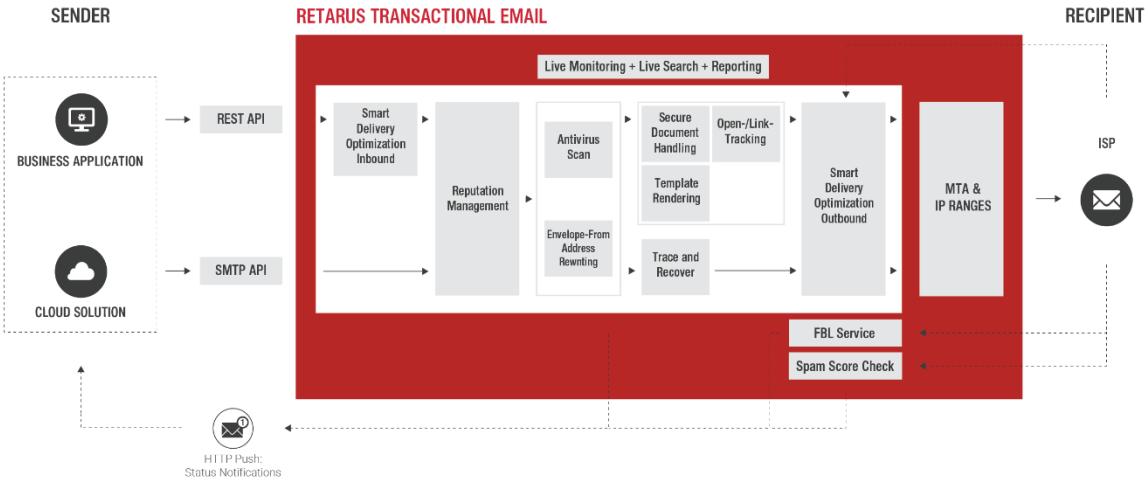
Data Loss Prevention examine les e-mails adressés à des destinataires externes par les utilisateurs du client afin de rechercher des modèles définis lors de la configuration, comme des numéros de carte de crédit ou des numéros de compte bancaire (IBAN). Lorsqu'un e-mail contient de tels modèles, la transmission aux destinataires externes est bloquée. En outre, des employés déterminés, comme un administrateur ou un chargé de conformité, peuvent être informés de la tentative d'expédition. L'e-mail en question est joint à la notification. Une option facultative permet d'informer l'expéditeur d'origine. La recherche de tels modèles comprend le corps de message. Les pièces jointes peuvent également être bloquées en fonction des extensions de fichier (par exemple, exe, mp3, zip) ou des types MIME utilisés. Par ailleurs, il est possible de n’autoriser l'envoi d'e-mails à des destinataires externes que lorsque les e-mails incluent une instance de contrôle (par exemple, une boîte de messagerie de fonction) dans la liste des destinataires.

E-Mail Infrastructure

Retarus Transactional Email

Grâce à **Retarus Transactional Email**, de grands volumes d'e-mails peuvent être envoyés directement depuis une application commerciale, sans surcharger l'infrastructure des e-mails propre au client. Pour ce faire, l'infrastructure du client sera connectée à Retarus Enterprise Cloud via des interfaces standard. Les données sont traitées par des centres de données propres à Retarus.

System Architecture Transactional Email



Interfaces

INTERFACES	REST (V2)	SMTP
Max. Volume Sent per Hour	Scalable as required	Scalable as required
Smart Delivery Optimization	✓	✓
Status Information for Each Email	API-Callback (Webhooks)	API-Callback (Webhooks)
Email Reporting (CSV)	✓	✓
Smart Network Data Services Reporting*	Upon request	Upon request
Reputation Management	• Dedicated IP (optional) • Blacklist-Monitoring • Live monitoring • SPF/DKIM • Suppression list • Registered Sender Domain • Feedback-Loop-Service* • CSA certified (EU, CH) • IPv6/IPv4 support	• Dedicated IP (optional) • Blacklist monitoring • Live monitoring • SPF/DKIM • Suppression list • Registered Sender Domain • Feedback-Loop-Service • CSA certified (EU, CH) • IPv6/IPv4 support
List Unsubscribe Header Support	✓	✓
Multi-Client Capability (Multi Domain Configuration)	✓	✓
IP-Whitelisting	✓	✓
Encrypted Connection to the Retarus System	✓	✓
Technical Requirements	HTTPS API client (job) and receiving web service (status)	Application with SMTP support (job) and receiving web service (status)
Open Tracking	✓	-
Link Tracking	✓	-
Envelope From Address Rewriting	✓	✓
Outbound AntiVirus MultiScan	✓	✓
Secure Document Handling	✓	-
Template rendering	✓	-
Trace and Recover	-	✓
Spam Score Check	✓	✓
EAS Live Monitoring	✓	✓
EAS Live Search	✓	✓
EAS Reporting	✓	✓
Max. Mail Size	20 MB	20 MB

* Ces fonctionnalités requièrent l'utilisation d'adresses IPv4.

Configuration du service de base

La configuration du service de base comprend des codes d'accès, une IP d'authentification enregistrée pour un point d'arrivée EPI ou un serveur SMTP dans un centre de données de Retarus. La communication s'effectue en utilisant une connexion sécurisée via HTTPS et/ou SMTP Auth Basic via eTLS. La configuration comprend un domaine/une adresse d'expéditeur, les paramètres du poste par défaut, le routage IP, l'enregistrement SPF et la signature DKIM. Le compte sera activé une fois qu'il sera totalement et correctement configuré et une description de l'interface sera fournie.

*Clarification on IPv6 address: The use of the following functionalities with the services require using IPv4 addresses:

- Smart Network Data Services reporting
- Feedback-Loop-Service
- CSA-certified IP areas (Certified Senders Alliance)

Dedicated IP

Un ou plusieurs domaines expéditeurs seront affectés à une adresse Dedicated IP. Cela permet aux circulations des e-mails de différentes applications d'être isolées, aux sociétés mères/filiales d'être séparées et aux régions d'être divisées. L'utilisation d'une Dedicated IP est recommandée si un minimum d'un million d'e-mails est envoyé par mois. Étant donné que le service Transaction Email est généralement connecté à un groupe de centres de données (actif/actif), l'utilisation d'une Dedicated IP requiert au moins deux adresses Dedicated IPs. Une fois que les adresses Dedicated IPs seront configurées, Retarus fournira des adresses IPv4 au client pour utilisation pendant la durée du contrat. Elles seront intégrées au système Blacklist Monitoring de Retarus. Retarus peut changer l'adresse IP à tout moment.

Enforced TLS

Pendant la configuration de base du service, il sera déterminé au niveau du domaine expéditeur si un protocole encryption hybride sera utilisé pour chaque e-mail envoyé. Ce faisant, nous entendons configurer une connexion cryptée dès que le client envoie des e-mails via le domaine donné (enforced TLS). Si la connexion cryptée est refusée du côté du destinataire, le processus d'envoi sera annulé.

Envelope From Address Rewriting

Facultativement, Retarus propose une Envelope From Address Rewriting pour les e-mails sortants afin de rediriger les éventuelles réponses à une boîte de réception dédiée. La réécriture de l'adresse est particulièrement utile si, par exemple, les politiques de l'entreprise ne permettent pas que des e-mails soient envoyés à l'Internet ouvert via le propre domaine de la société.

Account / Access Token

Un account est défini comme une unité d'authentification (définition du nom d'utilisateur/mot de passe API, etc.) et se rapporte à un centre de calcul spécifique, point d'accès API. Plusieurs domaines peuvent être gérés sous chaque compte. Il est également possible de gérer le même domaine sous plusieurs comptes.

Smart Delivery Optimization

Retarus utilise une gestion intelligente de l'envoi et de la réception des e-mails basée sur le domaine expéditeur. Smart Delivery Optimization adapte automatiquement le comportement d'envoi du client aux réponses des FSI et/ou des FSE individuels afin de maintenir le haut rendement du message pour les FSI et/ou FSE. Dans des cas exceptionnels, la gestion de l'expédition optimisée peut entraîner une réduction de la capacité de traitement accordée.

Status Information via API Callback (Webhook)

Grâce à API Callback (Webhook), Retarus fournit des informations de statut pour chaque e-mail envoyé. Le client sera informé des évènements récemment créés, tels que le statut de distribution, les raisons de non-distribution, le blocage d'e-mails adressés aux destinataires inclus dans la Suppression List, ainsi que les informations d'Open Tracking et de Link Tracking. En utilisant la publication http, les informations de statut peuvent être intégrées automatiquement aux processus et aux applications de l'entreprise. Ainsi, Retarus soutient la propreté des bases de données ainsi que le Bounce and Traffic Management actif du client, promouvant donc durablement la réputation des propres domaines du client.

Retarus EAS – Live Monitoring

Retarus fournit une surveillance en direct via le Portail EAS qui permet le suivi des e-mails envoyés en temps réel. Grâce à cette solution, les évolutions des tendances dans la distribution, les rebonds durs et souples, ainsi que les messages abandonnés peuvent être détectés et des contre-mesures peuvent être prises.

Retarus EAS – Live Search

EAS Live Search de Retarus fournit un aperçu transparent de vos e-mails envoyés. EAS Live Search vous permet de rechercher des e-mails sortants par périodes de temps, ID de messages, expéditeurs et destinataires, et de recevoir des informations de statut détaillées des 45 jours précédents.

Retarus EAS – Reporting

EAS Reporting de Retarus vous donne un aperçu transparent des e-mails envoyés au cours des 45 jours précédents, qui est téléchargeable sous format de fichier CSV ou Excel (XLSX).

Smart Network Data Service – Report (SNDS)

Smart Network Data Service (SNDS) vous fournissent les données dont vous avez besoin pour comprendre votre réputation chez Microsoft et l'améliorer. Le SNDS vous donne accès à des données détaillées sur l'adresse IP que vous utilisez, sous format de fichier CSV. Ce service peut être utilisé uniquement en combinaison avec une adresse Dedicated IP.

E-Mail Reporting (CSV)

Retarus offre un rapport de distribution sous format CSV via le portail Enterprise Administration Services Portal (EAS) Ces rapports sont disponibles pour le client quotidiennement et pour une période de 180 jours. Ces rapports incluent uniquement les transactions ayant un statut final. Les transactions qui sont encore en cours de traitement ne sont pas répertoriées. Ce rapport est accessible en plusieurs fichiers ou en fichier compressé (par ex., comme fichier ZIP).

Veuillez noter : La configuration d'un rapport CSV nous oblige à stocker temporairement les données à des fins de prestation du service. Les données stockées comprennent des informations sur le traitement du message, ainsi que des données personnelles, telles que les adresses électroniques des expéditeurs et des destinataires, mais pas des données sur le contenu.

Retarus Spam Score Check

La probabilité de classement de messages comme spams dépend de plusieurs facteurs. Un formatage HTML ou des structures de tableau inhabituels, un nombre excessif de liens ou des mots douteux utilisés dans l'objet ou le corps du texte peuvent déclencher un avertissement contre les spams. À cet effet, Retarus offre un service Spam Score Check payant. Cela vous permet de vérifier la probabilité que votre e-mail soit classé comme spam, avant de l'envoyer. Le Spam Score est renvoyé via un processus automatisé qui transmet les informations déterminées de Retarus par e-mail à votre adresse de réponse fournie, ou via API Callback à votre service web disponible. Une fois la transmission effectuée, toutes les informations en rapport avec cette transmission sont supprimées et ne seront pas stockées.

Open Tracking et Link Tracking (CNAME optionnel)

Open Tracking vous permet de déterminer le taux d'ouverture des e-mails, tandis que Link Trading vous permet de déterminer le taux d'ouverture des liens contenus dans les e-mails. Pour ce service, le corps de l'e-mail ou le lien respectifs seront modifiés afin que les messages puissent être analysés. Afin de réduire la possibilité que vos e-mails soient classés comme spams, Retarus recommande d'utiliser le service CNAME. Cela permet au client d'utiliser un de ses propres (sous-)domaines. Le client configure un enregistrement A dû (sous-)domaine sur l'adresse du serveur de Retarus. Le client doit informer les destinataires respectifs des e-mails de l'utilisation d'Open Tracking et de Link Tracking dans une déclaration de confidentialité appropriée et il doit obtenir leur consentement préalable si nécessaire, conformément aux lois applicables.

AntiVirus MultiScan

Retarus vérifie si les messages contiennent des virus pendant le processus d'envoi. Le client peut déterminer préalablement si seuls les pièces jointes et/ou le corps d'un e-mail doivent être vérifiés à la recherche de menaces. Cette vérification se fait à l'aide de deux scanners antivirus de différents fournisseurs sélectionnés par Retarus. Dès que ces fournisseurs proposeront des mises à jour ou de nouvelles versions, Retarus les utilisera aussi rapidement que possible pour la détection de virus. Si un virus est détecté dans un e-mail, Retarus supprime l'e-mail infecté. Les informations de statut des e-mails infectés seront fournies au client via API Callback (Webhook).

Secure Document Handling

Les fichiers joints aux e-mails envoyés peuvent être cryptés grâce à Secure Document Handling. Dans ce but, les pièces jointes seront automatiquement compressées dans une archive ZIP protégée par mot de passe dans l'infrastructure de Retarus avant l'envoi. Les mots de passe seront fournis aux destinataires dans des e-mails différents. Afin d'offrir la meilleure protection possible à votre destinataire, le service est uniquement disponible en combinaison avec notre service Outbound AntiVirus MultiScan.

Trace and Recover

Cette fonction indique comme messages Trace & Recover les e-mails envoyés via une connexion SMTP. Les messages marqués par Trace & Recover sont stockés dans un stockage à court terme pour une période de 45 jours et peuvent être localisés, durant cette période, grâce à la fonction Retarus EAS Live Search. Pour les messages marqués, un aperçu des 1 000 premiers caractères est disponible. Avant de pouvoir renvoyer un message, si nécessaire, seul le destinataire initial peut être modifié.

La fonction supplémentaire Trace & Recover requiert AntiVirus MultiScan et est activée par Retarus pour un compte technique que le client doit déterminer. Trace & Recover ne peut pas être utilisé en relation avec Envelope-From Address Rewriting (sortant).

Processing Capacity

Les capacités de traitement sont calculées en utilisant la configuration de base de Transactional Email. Cela suppose une taille d'e-mail de 200 kilo-octets et comprend Open et Link Trading pour une période d'une heure. La capacité de traitement est calculée systématiquement pour chaque minute pendant une heure. Tenant compte de l'éventualité de pics d'envois, la capacité de traitement réelle peut être de 1,25 fois la capacité de traitement convenue. Dans le cas de caractéristiques supplémentaires ou d'e-mails plus longs, la bande passante peut baisser. Une augmentation de la capacité de traitement permet au client d'atteindre une performance par heure plus importante. Il s'agit de la performance maximum pour le traitement des messages avec Retarus. Des divergences sont possibles. Afin d'augmenter la capacité de traitement, des contrôles d'exigence individuelle sont nécessaires.

Exemple : Capacité de traitement

Dans l'exemple suivant, la capacité de traitement contraactuellement convenue est de 150 000 emails/heure :

- (150 000 emails/heure) / (12 x intervalle*/heure) = 12 500 emails/intervalle*
- L'extension maximale pour les pics d'envoi de 25% peut augmenter le débit jusqu'à un maximum de 15 625 emails/intervalle*

*Un intervalle est de 5 minutes.

IP Whitelisting

L'utilisation de la fonction Whitelisting de Retarus vous permet d'améliorer la sécurité de votre « distribution permise ». Vous définissez expressément quelles applications de votre réseau peuvent utiliser ou non le service Transactional Email.

Feedback Loops

Retarus communique avec différents fournisseurs de service Internet en utilisant un accord de plainte. Les informations d'une plainte seront reportées à Retarus par les FSI impliqués dans le formulaire des boucles de rétroactions (ARF).

Les boucles de rétroaction sont un mécanisme fourni par le FSI pour informer les expéditeurs dès que leurs messages sont classés comme indésirables. « Indésirable » fait référence à votre message classé comme spam par le destinataire de l'e-mail (par ex., en cliquant sur « Ceci est un spam » dans sa propre boîte de réception).

La rétroaction de la plainte est effectuée avec un processus automatisé, dans lequel les informations de la plainte transmises sont lues et commentées par e-mail à votre adresse électronique de réponse ou via API Callback à votre service web disponible. Une fois la transmission effectuée, toutes les informations en rapport avec la plaine sont supprimées et ne seront pas stockées.

Billing

Les e-mails sont facturés à l'unité, une unité correspondant à 200 kilo-octets. Pour le règlement, les e-mails supérieurs à 200 kilo-octets seront divisés en plusieurs unités.

Exemple : Un e-mail est de 2 403 kilo-octets (environ 2,4 Mo) équivaut à 13 unités à facturer.

Les e-mails sont facturés (identifiant : ID de l'e-mail) que la transmission soit réussie ou pas (par ex., si les e-mails sont bloqués ou distribués).

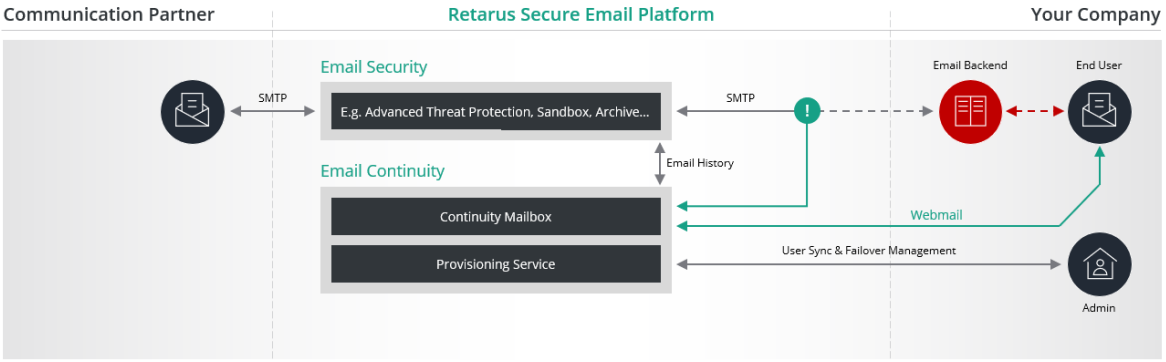
Retarus Email Continuity

Retarus Email Continuity est une plateforme de messagerie alternative pour maintenir la communication par e-mail en cas de scénario catastrophe (par ex. infiltration de logiciels malveillants, défaillance du centre de données, panne du Cloud). Si nécessaire, la réception et l'envoi de tous les e-mails entrants et sortants sont acheminés via cette plateforme à la demande du client.

Autres fonctionnalités :

- Accès de l'utilisateur final à la boîte aux lettres de Email Continuity via webmail (HTTPS)
- Fonctionnalité d'annuaire interne pour afficher et retrouver toutes les informations de contact transmises au sein du domaine client concerné
- Accès administratif au service Continuity via REST API pour la gestion de la continuité des boites mails utilisateurs
- Configuration de la boîte aux lettres via synchronisation d’annuaire (fichier au format csv)
- Notification automatique des nouveaux utilisateurs de Continuity
- Portail de gestion des mots de passe (via tokens gérés par le client)
- Possibilité de retransmission des emails de la boîte aux lettres de Continuity (Backsync) vers l'environnement de production
- Accès optionnel à tous les messages entrants des derniers jours (historique des emails jusqu'à 14 jours) en fonction des domaines attribués au client. Pour cela, une référence aux enregistrements MX spécifiques du client vers l'infrastructure Retarus est nécessaire

Architecture du système Email Continuity



Retarus Predelivery Logic

Grâce à la logique de pré délivrance de Retarus, le traitement des messages au sein de l'infrastructure de Retarus est influencé, avant la livraison à l'infrastructure spécifique du client

La configuration du client s'effectue en créant des règles individuelles dans le portail EAS, composées de "conditions" et "d'actions". Par exemple, le routage et la réécriture peuvent être effectués sur la base de certaines informations d'en-tête telles que l'expéditeur, l'utilisateur ou l'objet du message.

Connexion à Retarus

La connexion des systèmes du client à l'infrastructure Retarus est généralement établie à l'aide du protocole de chiffrement Internet TLS (Transport Layer Security) afin de garantir une transmission sécurisée des données via SMTP. Selon la configuration choisie, il est également possible d'opter pour les protocoles TLS opportuniste, TLS forcé ou une connexion via un réseau virtuel privé (VPN).

La condition préalable à une connexion via VPN est une connexion simultanée aux deux centres de données Retarus de Munich et Francfort-sur-le-Main (RZ DE 1 et RZ DE 2).

Remarques

La protection contre les messages entrants et sortants potentiellement malveillants et contre les liens intégrés et les pièces jointes repose essentiellement sur des méthodes statistiques et d'approximation. Même en cas de mise en œuvre de l'ensemble des caractéristiques de performance, il peut arriver que des messages soient rejetés ou signalés par erreur, ou que des messages potentiellement malveillants soit distribués au client.

En outre, Retarus signale que la procédure de quarantaine, indépendamment de la manière dont est utilisée la messagerie et des configurations définies par le client, est susceptible d'entraîner une non distribution ou un retard de distribution de certains messages, en particulier les messages dits « faux positifs », ce qui risque de porter préjudice au client.

Les options de services suivantes requièrent Antivirus MultiScan 4x :

- Deferred Delivery Scan
- Sandboxing
- Time-of-Click Protection
- Patient Zero Detection

Sauf convention contraire expresse par écrit, l'utilisation de Retarus Email Encryption se limite à la communication de l'entreprise générée personnellement. Le traitement des messages générés par une machine et/ou une application nécessite que l'utilisateur de Retarus Email Encryption soit un utilisateur eBusiness.

Implementation, Change-Management and Support

La mise en œuvre commence après l'adjudication du contrat et la remise des fiches de configuration totalement et correctement remplies par le client.

Pour les questions de support et de service client, ainsi que pour les demandes de changement, le client doit informer Retarus du cercle des personnes autorisées qui peuvent officiellement faire de telles demandes ou poser de telles questions. Le contact technique du client pour la mise en œuvre du service est généralement établi comme le premier point de contact autorisé pour des questions dont les réponses sont confidentielles. En tant qu'administrateur client, il peut ensuite saisir d'autres contacts de support dans le portail EAS et les autoriser. Les administrateurs clients peuvent modifier, ajouter ou supprimer ces autorisations à tout moment.

Les modifications du service et les solutions aux incidents (y compris les solutions de contournement) mises en œuvre dans la commande du client doivent être acceptées par le client au moins sous forme de texte. Si le client n'a pas répondu dans les 10 jours, le ticket du client concerné sera automatiquement fermé à l'issue de cette période et la modification/solution sera considérée comme acceptée.

Duties of Cooperation

Le client est informé du fait qu'une utilisation correcte des services de Retarus et la qualité des services fournis dépendent considérablement de la coopération du client. Par conséquent, le client renverra la Fiche de mise en œuvre remplie, laquelle lui a été fournie lors de la conclusion du contrat, dans les cinq (5) jours ouvrables, respectera tout spécialement les devoirs de coopération établis dans le présent document et reconnaît que Retarus peut prendre des mesures techniques bénéfiques pour sécuriser la prestation d'un service stable et la réputation des fournisseurs de services Internet (FSI) des parties. Pour ce faire, Retarus a la permission expresse d'ignorer des commandes pour e-mails spécifiques, de restreindre le volume ou, dans des cas extrêmes, d'interdire l'accès. Si des efforts et/ou des coûts résultent du non-respect des devoirs de coopération, ceux-ci devront être couverts par le client.

Le client s'engage à envoyer des e-mails uniquement aux destinataires qui, conformément au cadre juridique applicable, l'ont expressément autorisé à le faire (Opt-In), ou pour lesquels il existe une autre autorisation légalement reconnue pour ce faire.

Email Design

Chaque e-mail doit inclure une empreinte dans le corps du texte, devant respecter les exigences légales applicables et être facilement reconnaissable.

De plus, les clauses suivantes s'appliquent à l'envoi d'e-mails au contenu promotionnel :

- L'expéditeur d'un e-mail publicitaire doit être clairement visible.
- Dans chaque e-mail, le destinataire doit être informé distinctement qu'il peut révoquer à tout moment son consentement à recevoir des e-mails. La révocation/annulation des e-mails (Opt-Out/Unsubscribe) doit généralement être facile à effectuer par le destinataire, c'est-à-dire sans avoir à saisir de données d'accès (par ex., identifiant ou mot de passe).
- L'en-tête ou l'objet d'un e-mail ne doit pas masquer ou cacher l'expéditeur ni la nature commerciale de l'e-mail. Dans ce cas, masqué ou caché signifie que l'en-tête ou l'objet sont volontairement conçus de manière à ce que le destinataire ne reçoive pas d'informations ou reçoive des informations purement mensongères quant à la véritable identité de l'expéditeur ou à la nature commerciale du message avant de lire le contenu du message.

Technical Configuration

- Les adresses de l'expéditeur doivent être enregistrées et font partie de l'administration du service. L'adresse de l'expéditeur doit être en mesure de recevoir des e-mails (enregistrement DNS MX valide). Le domaine de l'expéditeur doit également avoir un enregistrement A DNS valide. Les adresses de l'expéditeur basées sur des rôles (par ex., abuse@ ou postmaster@) ne sont pas autorisées.
- Le client doit immédiatement supprimer les adresses e-mail des listes de mailing correspondantes s'il est découvert que l'adresse n'existe pas après la distribution et, au plus tard, si trois rebonds durs ont eu lieu. Le taux total de rebonds durs par FSI ne doit normalement pas dépasser 1 %. Les adresses du destinataire basées sur des rôles (par ex., postmaster@, abuse@) seront supprimées.
- Le client doit supprimer les adresses e-mail des listes de mailing correspondantes si le destinataire classifie l'e-mail comme spam et le signale (plainte) ou s'il révoque son consentement à recevoir des e-mails.
- Pour l'adresse « MAIL FROM » incluse dans la communication SMTP entre les serveurs électroniques, un enregistrement SPF-From doit être saisi, ce qui permet d'effectuer un test SPF du côté du destinataire. L'enregistrement SPF doit se terminer par « -all » ou « ~all ». Si les

saisies nécessaires ne sont pas effectuées du côté du client dans les dix (10) jours ouvrables, le nouveau contrôle sera facturé en tant qu'effort.

- Le client doit toujours utiliser le processus DKIM (DomainKeys Identified Mail). Pour chaque domaine expéditeur enregistré pour le client auprès de Retarus, le client doit fournir une clé DKIM dans son DNS. Si les saisies nécessaires ne sont pas effectuées dans les dix (10) jours ouvrables, le nouveau contrôle sera facturé en tant qu'effort.
- Un « List-unsubscribe »- header ou un « List-help »-header (voir RFC 2369) doit être inclus dans chaque e-mail envoyé. Un « List-unsubscribe »- header est nécessaire pour les envois basés sur des listes et doit être inséré avec un « POST HTTPS » link comprenant une fonction « One-click unsubscribe » (RFC 8058). Ce lien fourni doit entraîner une désinscription directe en un clic, au moins au niveau de la liste. L'expéditeur peut envoyer une confirmation à l'utilisateur une fois la désinscription effectuée. Dans les envois non basés sur des listes, un « List-help » header doit être inclus au lieu de « List-unsubscribe »- header. Un « List-help »-header doit comporter au moins une adresse « mail-to » ou un HTTPS link. Les http links ne sont pas autorisés. L'utilisation de l'adresse « mailto: » et du HTTPS link doivent permettre au destinataire de recevoir des informations sur la raison pour laquelle l'e-mail lui a été envoyé et sur les raisons pour lesquelles la désinscription au niveau de la liste n'est pas possible.

- L'utilisation de l'en-tête « list-unsubscribe-Post »-Header requiert une adresse URL valide pouvant recevoir et traiter ces demandes POST.

  Exemple :

```
List-Unsubscribe:      <mailto:listrequest@example.com?subject=unsubscribe>,
                       <https://example.com/unsubscribe.html?opaque=123456789>
List-Unsubscribe-Post: List-Unsubscribe=One-Click
```

- Des exceptions à cette obligation peuvent être faites s'il n'est pas possible de se désabonner des e-mails dans le sens susmentionné en raison de la conception du service et de l'envoi d'e-mails automatisés associé.
- Le Client doit mettre en place une adresse e-mail abusive pour le signalement de l'abus des adresses e-mail des destinataires des e-mails et la surveiller. L'adresse email d'abus peut être configurée par exemple comme abuse@domain.
- La livraison des e-mails au service Retarus Transactional Email doit se faire via Transport Layer Security (TLS - opportunistic/enforced) du client, selon l'état actuel de la technique. Retarus utilise pour l'envoi des e-mails au destinataire le Transport Layer Security (TLS) en utilisant les adresses IP CSA.
- Retarus est certifié CSA (« Certified Senders Alliance »). Les obligations de collaboration décrites dans les présentes reflètent les exigences actuelles de la CSA. La CSA peut adapter ses exigences à tout moment. Par conséquent, le client s'engage à respecter lesdits changements. Le client en sera informé par Retarus.