Descripción de servicios y obligaciones de colaboración Retarus Secure Email Platform

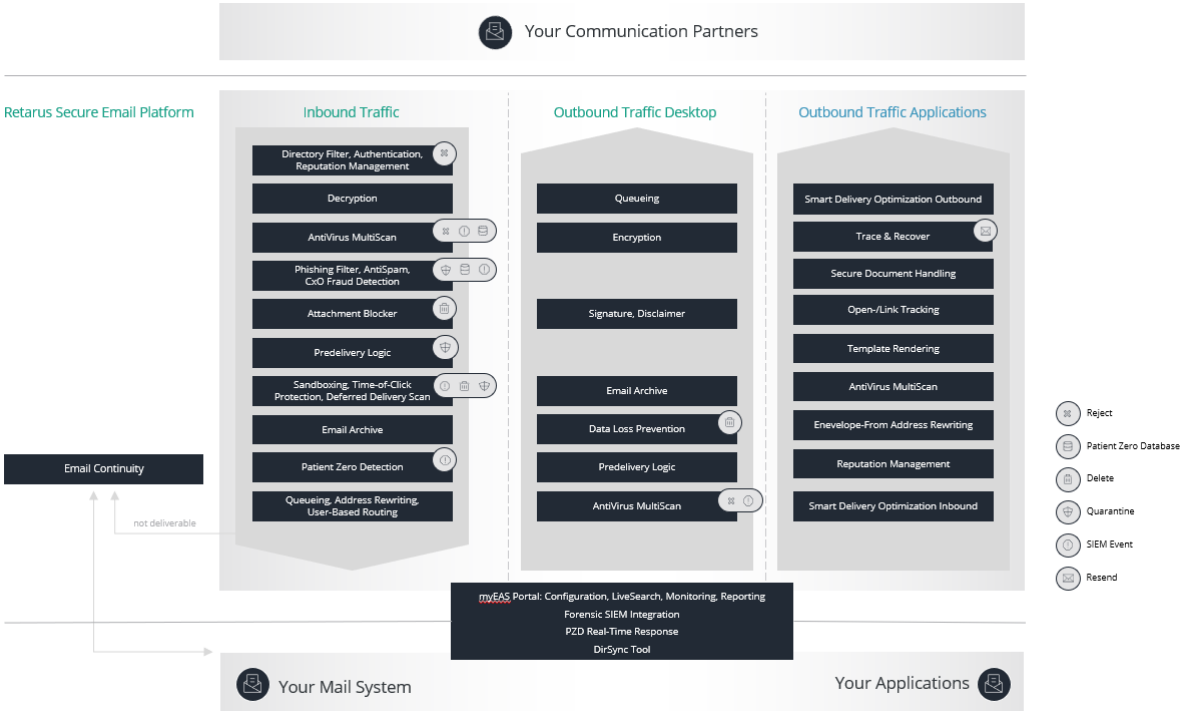
Retarus Secure Email Platform combina mecanismos de protección completos, Advanced Threat Protection y la característica patentada de Postdelivery Protection Patient Zero Detection® junto con las siguientes funcionalidades adicionales: Dynamic Email Routing, Email Encryption y Email Continuity.

Las aplicaciones de negocio también pueden conectarse a la plataforma a través de los módulos de correo electrónico transaccional de Retarus.

La gama de servicios está estructurada en las siguientes categorías principales: **Email Cloud Gateway, Email Security, Email Compliance y Email Infrastructure.**

Contenido

Arquitectura del sistema Secure Email Platform



Email Cloud Gateway

Retarus Email Security protege las infraestructuras de correo electrónico contra todo tipo de malware, como virus, spam, correos phishing, ransomware y demás ataques digitales. Los métodos de filtrado en varias fases se actualizan y optimizan continuamente. El procesamiento de datos tiene lugar en centros de datos propios de Retarus conforme a las reglas de protección de datos aplicables.

El Email Cloud Gateway incluye las siguientes funcionalidades:

Directory Filter / Reputation Management

El Directory Filter rechaza conforme al RFC (método Reject) aquellos correos electrónicos que están dirigidos al destinatario pero no están configurados en el Retarus Enterprise Administration Services Portal (portal EAS). La configuración y actualización pueden realizarse manualmente por el propio cliente mediante el propio portal EAS o de forma automatizada mediante Directory Synchronization en un formato especificado por Retarus con libretas de direcciones y directorios del cliente.

La reputación de los remitentes de los correos electrónicos entrantes se comprueba a través de la gestión de la reputación de entrada, que complementa el filtrado de directorio. La autorización de un remitente se valida mediante los mecanismos SPF (Sender Policy Framework) y DKIM (DomainKeys Identified Mail). En caso de que falle la validación de los correos electrónicos clasificados, dichos correos se gestionan de acuerdo con la configuración del cliente en el portal EAS o, si el cliente lo ha activado, se procesan posteriormente de acuerdo con la especificación de la política DMARC (Domain-based Message Authentication, Reporting & Conformance) del propietario del dominio (remitente) (acciones: Ninguna, Cuarentena, Rechazo).

Nota: El uso de DMARC requiere el enrutamiento a un registro MX dedicado de Retarus.

AntiVirus Multiscan 2x

Retarus analiza los mensajes entrantes y (si así se acuerda) los mensajes salientes en busca de virus. Para realizar estos análisis, Retarus utiliza dos detectores de virus de su elección de diferentes proveedores. Tan pronto como haya actualizaciones o lanzamientos de estos proveedores, Retarus los utilizará para buscar virus inmediatamente. Si se detecta un virus, Retarus eliminará todos y cada uno de los correos electrónicos infectados. Los destinatarios de los correos infectados o sus administradores guardados para tal ocasión serán informados como parte de la gestión de la cuarentena.

Protección DHA

Protección contra ataques de recolección de directorios (DHA) para los dominios de correo electrónico seleccionados por el propietario del dominio. Los mensajes dirigidos a destinatarios no válidos dentro del dominio en cuestión serán rechazados. La recepción de mensajes a destinatarios no válidos se limitará mediante técnicas de reducción de la capacidad de entrega de los remitentes de estos mensajes.

Backscatter Protection

Protección contra el uso indebido de los mensajes de rebote generados automáticamente mediante técnicas de Backscatter.

El Backscatter es el uso no autorizado de la dirección de correo electrónico válida de otra persona para campañas de spam. Puede darse el caso de que el servidor de correo electrónico receptor de los destinatarios reciba un gran número de notificaciones de estado de entrega (por ejemplo, si la dirección receptora no existe) en la dirección de correo electrónico válida de la persona que fue utilizada como remitente sin su conocimiento. Los correos electrónicos no se entonces entregan al remitente real.

Gracias a la protección Backscatter, un mayor número de estos mensajes generados automáticamente serán identificados y filtrados, y se impedirá su entrega mediante el aislamiento del destinatario en cuestión en la cuarentena personal. En la cuarentena personal, estos mensajes se marcarán como Spam NDR.

Email Back-Up / Queuing

En caso de no poder entregar los mensajes destinados al cliente, Retarus almacenará los mensajes entrantes durante un máximo de 96 horas. En caso de que no pueda resolverse la imposibilidad de entrega, el remitente del mensaje recibirá un aviso de imposibilidad de entrega por correo electrónico. Retarus intentará realizar la entrega en intervalos cortos regulares a lo largo de este lapso de 96 horas. Si la imposibilidad de entrega finaliza dentro de este plazo, Retarus reenviará los mensajes entrantes por lotes.

Large Email Handling

El cliente puede definir limitaciones de tamaño para los mensajes de correo electrónico voluminosos entrantes; de modo que los mensajes que superen dicho tamaño no se envían directamente a los buzones de correo del cliente, sino que se ponen a disposición en forma de descarga a través Retarus. Si así se ha configurado, el destinatario recibe una notificación sobre la recepción de un correo de gran tamaño. La descarga tiene lugar a través de un enlace HTTP con autenticación del usuario simplificada (OneClick-Token-Login).

User based Routing

En el marco del enrutamiento basado en usuarios, Retarus entrega a servidores de destino específicos mensajes de correo electrónico para destinatarios definidos del cliente dentro de un dominio.

Email Signature / Disclaimer

El cliente tiene la posibilidad de crear firmas o descargos de responsabilidad en el Enterprise Administration Services Portal (portal EAS). Retarus adjuntará a los mensajes de correo electrónico salientes del cliente las firmas o los descargos de responsabilidad creados mediante el portal EAS. En caso de utilizarse caracteres comodín, estos se rellenan con datos procedentes de Directory Synchronization.

Email Live Search

Email Live Search permite realizar un seguimiento en tiempo real de todos los mensajes entrantes y salientes. De este modo se puede averiguar si un mensaje de correo electrónico concreto estaba infectado (y, en su caso, por qué virus) y qué otros filtros y reglas se aplicaron.

Access Management

En el Retarus Enterprise Administration Services Portal (portal EAS) se pueden asignar derechos de acceso para administradores concretos conforme a las especificaciones del cliente, p. ej. con distintos derechos de acceso para determinados países, sucursales, dominios o departamentos.

Email Security

Retarus Email Security protege a las infraestructuras de correo electrónico de malware como virus, spam, correos electrónicos, ataques de phishing, ransomware y otras amenazas. Los métodos de filtrado y las fuentes de datos de malware se actualizan y optimizan constantemente. El procesamiento de datos se realiza en los centros de datos propios de Retarus, de acuerdo con las normas de protección de datos Europeas.

AntiVirus Multiscan 2x

Retarus scans incoming and – where agreed – outgoing messages for viruses. To carry out these scans, Retarus uses two virus scanners of their choosing from different providers. As soon as there are updates or releases from these providers, Retarus will use them for virus scans immediately. Should a virus be detected, Retarus deletes any and all emails infected. The respective recipients of the infected emails and/or their administrators saved for such an occasion, will be informed as part of quarantine management.

AntiVirus MultiScan 4x

Con las mismas funciones que el AntiVirus MultiScan doble, pero con cuatro exploradores antivirus de distintos proveedores para la detección de infecciones por virus.

External Sender Visibility Enhancement

External Sender Visibility Enhancement marca los mensajes entrantes que utilizan, en el remitente, un dominio de remitente atribuido al cliente. Para la validación del remitente, se utiliza el campo de encabezado MIME-FROM. Los mensajes entrantes se marcan, dentro de la infraestructura de Retarus, con iconos Unicode predefinidos (símbolos) antes de su traspaso a la infraestructura del cliente. La marca aparece en el campo del remitente (nombre descriptivo).

Antispam Management y Phishing Filter (inbound)

Los mensajes recibidos en Retarus y dirigidos al cliente son examinados por los filtros de spam utilizados por Retarus, provistos de una probabilidad de SPAM e identificados como “spam potencial” conforme a los valores umbral definidos de forma específica para el cliente. Los mensajes clasificados como “spam potencial” no se entregan de inmediato y se tratan conforme a la configuración en la gestión de cuarentena. De forma alternativa, los mensajes reconocidos como spam se pueden etiquetar y entregar (“tag and deliver”) si el cliente así lo desea. Para ello, Retarus utiliza diversos métodos y tecnologías de filtrado, muestreo y detección. El filtro de phishing especial coteja los enlaces contenidos en los correos electrónicos entrantes con fuentes especializadas en busca de direcciones URL de phishing conocidas. La toma de conocimiento y el tratamiento posterior de los mensajes puestos en cuarentena o etiquetados son competencia del cliente y de los usuarios designados por este.

Antispam Management y Phishing Filter (outbound)

Al igual que la gestión antispam y el filtro antiphishing de Retarus (entrante), la contraparte saliente emplea la renombrada tecnología de filtro antispam utilizada por Retarus. A cada correo electrónico saliente se le asigna una puntuación de probabilidad de SPAM, y los que superan un umbral configurable (fijado por defecto en el 60 %) están sujetos a diferentes opciones de eliminación en función de sus preferencias de configuración. Las opciones disponibles incluyen el rechazo, el fallo temporal (tempfail) o el descarte silencioso, lo que le permite adaptar la respuesta para alinearla con sus políticas de seguridad específicas. La flexibilidad de configuración se extiende a todos los niveles jerárquicos, lo que le permite ajustar con precisión la configuración a nivel de cliente, dominio, perfil y usuario. Para activar la función, póngase en contacto con el equipo de asistencia de Retarus.

Attachment Blocker

La entrega de determinados archivos adjuntos a correos electrónicos puede bloquearse conforme a las configuraciones del cliente. Mediante extensiones de archivo (p. ej. exe, mp3, zip) y según el tipo MIME correspondiente, se pueden determinar los archivos adjuntos que se quieren bloquear. El archivo adjunto a un correo electrónico entrante se elimina y tan solo se entrega al destinatario el contenido del correo electrónico, o bien se envía a un buzón de correo predefinido (p. ej. administrador) una copia del correo electrónico original con el archivo adjunto. Por medio de notificaciones configurables es posible informar a los destinatarios sobre la eliminación de archivos adjuntos.

Outbound Recipient Restriction

Por defecto, los correos electrónicos salientes procesados por Retarus pueden tener hasta 600 direcciones de destinatarios. Si un correo electrónico supera este umbral, Retarus lo rechaza para los destinatarios que lo superen, y la notificación depende de la configuración de su servidor de correo electrónico. Nuestra función de restricción de destinatarios salientes le permite establecer un número máximo personalizado de destinatarios (0-600) para los correos electrónicos salientes. Superar el límite configurado puede desencadenar un rechazo, un fallo temporal o un descarte silencioso según sus preferencias. Esta funcionalidad tiene como objetivo limitar los destinatarios, evitar la exposición de la identidad y facilitar una administración eficaz. La función puede configurarse en todos los niveles jerárquicos (cliente, dominio, perfil, usuario). Para activar esta función, se requiere inicialmente la ayuda del equipo de asistencia de Retarus.

Outbound Size Restriction

Por defecto, los correos electrónicos salientes procesados por Retarus pueden tener un tamaño de hasta 250 MB (256 000 kB). La función "Restricción del tamaño de salida" le permite restringir aún más el tamaño de los correos electrónicos salientes (outbound), si es necesario. Superar el límite configurado puede desencadenar un rechazo, un fallo temporal o un descarte silencioso según sus preferencias. La función puede configurarse en todos los niveles jerárquicos (cliente, dominio, perfil, usuario). Para activar esta función, se requiere inicialmente la ayuda del equipo de asistencia de Retarus.

Deferred Delivery Scan

En el marco del Deferred Delivery Scan (DDS), archivos adjuntos específicos son sometidos a un reanálisis mediante procesos de exploración adicionales. Mediante los nuevos análisis con las firmas actualizadas, se puede evitar con mayor probabilidad la entrega de contenidos maliciosos que no se hayan podido detectar durante el primer análisis. En caso de detectarse una infección por virus, Retarus elimina los mensajes afectados e informa según la configuración en la gestión de cuarentena. Puesto que DDS realiza una entrega demorada de los correos electrónicos entrantes, en ciertos casos no se aplican los niveles de servicio acordados relativos a los plazos de entrega.

Time-of-Click Protection

Se reescriben automáticamente los enlaces incluidos en mensajes de correo electrónico (URL rewriting). Cuando los destinatarios hacen clic en los correspondientes enlaces, se comprueba que estos no contengan direcciones de destino sospechosas de phishing. Si la página de destino no está identificada como página de phishing, se ejecuta una redirección directa. Si la página de destino es una página de phishing se muestra una advertencia de seguridad. Una vez finalizado el servicio, es posible que no se pueda acceder directamente a los enlaces correspondientes.

CxO Fraud Detection

CxO Fraud Detection utiliza algoritmos que identifican la suplantación de remitentes (from-spoofing) y la suplantación de dominios (domain-spoofing) para detectar direcciones de remitente falseadas (p. ej. de un superior de alto cargo). Los mensajes clasificados como fraude del CEO se tratarán conforme a la configuración en la gestión de cuarentena.

Sandboxing

Mediante el método de Sandboxing, los archivos adjuntos específicos se someten a un análisis más exhaustivo. Los adjuntos que puedan incluir contenidos maliciosos se ejecutan en una máquina virtual para detectar posibles comportamientos anómalos. Para esta comprobación, Retarus utiliza las soluciones de Sandbox de un proveedor especializado. En caso de detectarse una infección por contenidos maliciosos, los mensajes afectados se tratan conforme a la configuración en la gestión de cuarentena. Dado que, dependiendo entre otros factores del tamaño y el tipo del archivo y la cantidad de archivos adjuntos, el método de Sandboxing puede traducirse en una entrega demorada de los mensajes de correo electrónico entrantes, en ciertos casos no se aplican los niveles de servicio acordados relativos a los plazos de entrega.

Patient Zero Detection®

Patient Zero Detection® crea una huella dactilar digital (“hash”) de todos los archivos adjuntos y enlaces al recibirse los mensajes de correo electrónico dirigidos a los destinatarios del cliente. Si los antivirus utilizados por Retarus detectan con posterioridad contenidos maliciosos en un adjunto o enlace del mismo tipo, resulta posible identificar precozmente también a los destinatarios de mensajes potencialmente maliciosos ya entregados. En tal caso se informa de inmediato a los administradores del cliente y, en función de lo acordado, también directamente los destinatarios de dichos mensajes. Esto permite al cliente adoptar lo antes posible medidas para eliminar el código malicioso de su infraestructura o para evitar la propagación de código malicioso.

Patient Zero Detection® Real-Time Response

Con Patient Zero Detection® Real-Time Response, Retarus proporciona un software que el cliente podrá utilizar dentro de su infraestructura. Este software procesa automáticamente mensajes que, después de su entrega al buzón de correo del destinatario, han sido identificados como maliciosos gracias a Patient Zero Detection®. Posteriormente, estos mensajes pueden ser eliminados automáticamente del buzón de correo del destinatario. Para poder utilizar Patient Zero Detection® Real-Time Response, el cliente debe disponer de Retarus Forensic SIEM Integration y de una conexión a Microsoft Exchange. Para Patient Zero Detection® Real-Time Response se aplican unas condiciones de uso especiales que el cliente debe tener en cuenta y cumplir en caso de instalar o utilizar este software. Estas condiciones de uso están disponibles en el portal EAS.

Quarantine Management

En el marco de la gestión de cuarentena, el cliente o los usuarios que éste designe pueden definir la entrega de un informe de seguridad del correo electrónico (resumen) en momentos configurables de forma individual. Dependiendo de las opciones contratadas, el resumen contiene una sinopsis combinada de los mensajes de correo electrónico que fueron puestos en cuarentena o eliminados por Retarus a causa de correo gris (p. ej. boletines informativos), virus, spam, phishing, sandboxing, fraude del CEO, etc. durante el periodo definido. Los mensajes puestos en cuarentena pueden ser consultados por el cliente haciendo clic en la entrada correspondiente en el resume dentro del periodo definido (máximo 30 días). Si así lo ha configurado el cliente, los destinatarios individuales pueden acceder en línea a su cuarentena y personalizar sus ajustes. Los administradores del cliente pueden configurar ajustes de cuarentena válidos para todo el sistema en el Enterprise Administration Services Portal (portal EAS).

Forensic SIEM Integration

En el marco de la Forensic SIEM Integration, Retarus proporciona al cliente una interfaz para acceder a toda la información referente a incidencias y resultados (Event o Log) derivados del análisis de mensajes entrantes y salientes que se lleva a cabo mediante Retarus Email Security. El cliente puede integrar esta interfaz en una herramienta SIEM existente como fuente de datos adicional. Los eventos que se ponen a disposición del cliente están supeditados a las opciones contratadas y están disponibles para:

- AntiVirus Multiscan (Inbound y Outbound)
- Sandboxing
- CxO Fraud Detection
- Patient Zero Detection®
- Correos electrónicos salientes en general

Email Compliance

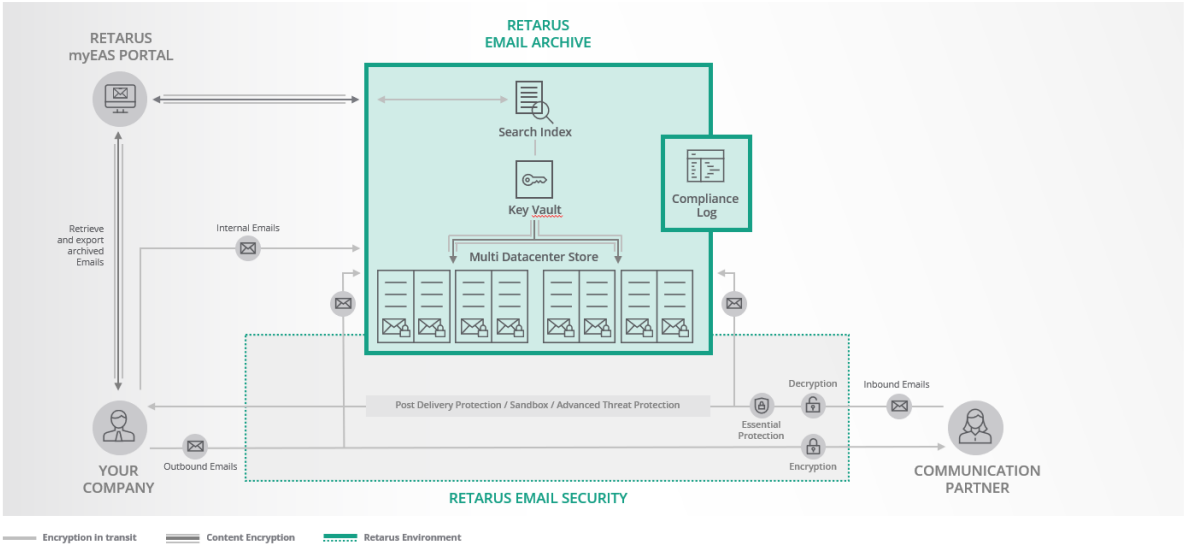
Retarus Email Archive

Retarus Email Archive guarda la comunicación por correo electrónico entrante y saliente, de forma automática, fiable y a largo plazo. Si es necesario, la comunicación interna por correo electrónico también puede guardarse en Retarus Email Archive.

Los mensajes entregados a Retarus Email Archive no se pueden editar, están protegidos contra el acceso no autorizado y son recuperables. Estos mensajes se almacenan durante la vigencia del acuerdo, por un máximo de diez años, y se eliminarán al final de la duración acordada en cumplimiento de la ley, a menos que se acuerde lo contrario. Durante el periodo de archivado, el cliente puede buscar y reenviar fácilmente los correos electrónicos archivados, utilizando diversas opciones de filtrado. Si el cliente desea exportar todo el archivo antes de que finalice el periodo de archivo acordado y se borren los correos electrónicos, deberá solicitarlo antes de que finalice el plazo.

El acceso del administrador al archivo de correo electrónico se basa en el principio de doble control. Los correos electrónicos archivados y los archivos adjuntos pueden encontrarse rápidamente utilizando potentes funciones de búsqueda que pueden restringirse de forma granular, si es necesario (por ejemplo, para cumplir requisitos de protección de datos).

Se creará automáticamente un protocolo de acceso completo.



Funcionalidades:

- Almacenamiento fiable a largo plazo de todos los correos electrónicos entrantes y salientes
- Almacenamiento de datos seguro y no editable basado en el cifrado híbrido
- Proporcionar información de seguimiento a través de EAS Live Search
- Protocolo de acceso creado automáticamente
- Ayuda a cumplir los requisitos reglamentarios
- Mensajes recuperables, incluidos los archivos adjuntos
- Acceso basado en el principio de doble control a través del portal web administrativo de Retarus
- Potente funcionalidad de búsqueda con opción de configuración para el cumplimiento de la protección de datos: búsqueda de correos electrónicos basada en el remitente, el destinatario o el formato del archivo adjunto; almacenamiento configurable de los datos (meta) para hacer búsquedas por asunto, texto completo o nombre del archivo adjunto

Opciones a petición

- Archivado de la comunicación interna por correo electrónico mediante Journaling (Microsoft Exchange o M365 Exchange Online)
- Acceso seguro y cómodo para los administradores del cliente mediante el inicio de sesión único
- Importación de correos electrónicos de otros sistemas de archivo (idealmente en formato EML)
- Exportación de correos electrónicos archivados a un sistema de almacenamiento de datos externo
- Utilización de las propias claves públicas del cliente (las claves privadas permanecerán en poder del cliente)

Retarus Email Encryption

Los servicios que ofrece **Retarus Email Encryption** ayudan a los clientes a garantizar la integridad, autenticidad y confidencialidad de los mensajes de correo electrónico. Para ello, antes de entregarse al destinatario, los mensajes de correo electrónico, incluidos los posibles archivos adjuntos, se cifran y/o firman automáticamente en el sistema de Retarus a través de normativas acordadas previamente o bien cuando así lo solicite el usuario. El análisis solicitado en busca de posibles virus se lleva a cabo antes del cifrado para los mensajes salientes y después del descifrado para los mensajes entrantes.

Funciones adicionales:

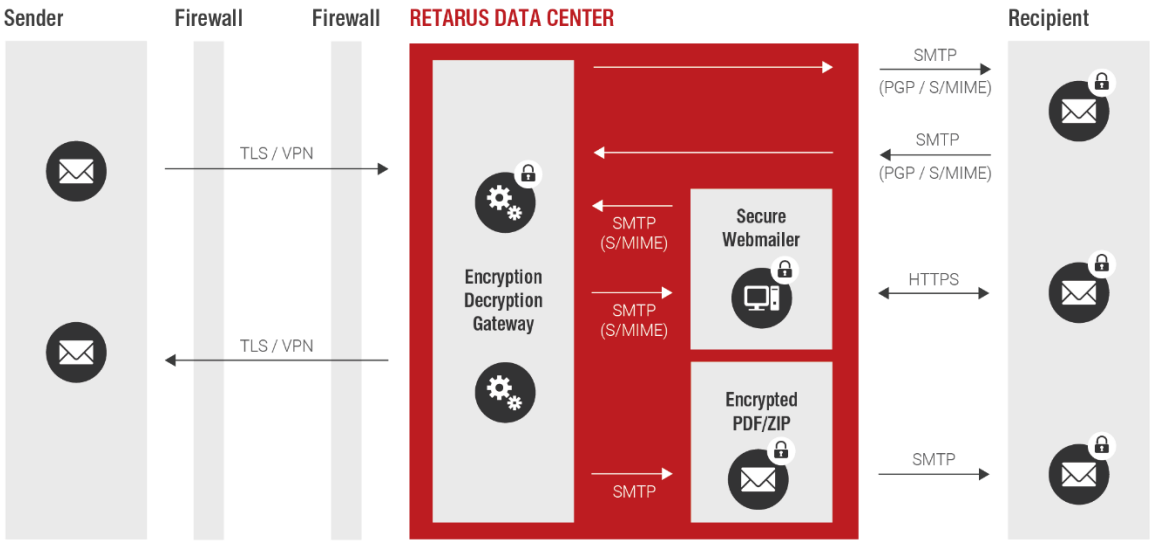
- Adopción de infraestructuras de claves públicas (PKI, por sus siglas en inglés) existentes
- Mayor uso de los certificados S/MIME existentes y válidos
- Compatibilidad con los estándares Open PGP, PGP y S/MIME
- Integración de las políticas de cifrado propias del cliente
- Suministro de complementos de Microsoft Outlook para controlar las acciones del usuario en relación con el cifrado o la firma de mensajes
- Prestación de formas alternativas de comunicación cifrada a través de Retarus Secure WebMailer o envío de archivos PDF o ZIP cifrados
- Integración opcional de un centro de confianza oficial (actualmente SwissSign) para crear certificados S/MIME según el estándar X.509
- Sincronización automatizada de usuarios para crear y renovar certificados (a petición)

User Synchronization for Encryption (USE

La sincronización de usuarios para el cifrado (USE) es una solución que simplifica la gestión de usuarios de cifrado, grupos y sus claves S/MIME o PGP asociadas. Con el objetivo de mejorar la experiencia del usuario y reducir la intervención manual, la USE automatiza el proceso de renovación, verificación y revocación de certificados y claves mediante la monitorización de las fechas de caducidad y la puesta en marcha de las acciones necesarias.

- Es capaz de importar de forma segura usuarios cifrados y asignarlos a grupos predefinidos.
- Gestiona las políticas en función de los requisitos de los clientes y los grupos de usuarios.
- Automatiza la creación/revocación y sincronización de S/MIME (SwissSign).
- Distingue entre certificados personales y de equipo para evitar interrupciones.
- Presenta una recertificación totalmente automatizada o semiautomatizada.
- Crea/elimina claves PGP y sincroniza las claves privadas correspondientes para cada usuario.
- Permite la importación de claves/certificados creados/comprados por separado por los clientes.
- La notación de reglas gestiona las políticas de cifrado específicas del cliente de forma legible para el ser humano.
- Es capaz de generar informes de sincronización e informes transaccionales S/MIME para el cumplimiento y la auditoría.
- Los informes pueden recibirse por correo electrónico o almacenarse en el SFTP compartido para su recogida.

Arquitectura del sistema Retarus Email Encryption



Digital Signature / Certificantes

Retarus Email Encryption permite firmar el correo electrónico saliente con claves PGP o certificados S/MIME a petición o automáticamente mediante normativas. Gracias a la información transparente, el usuario puede reconocer fácilmente el resultado de la verificación de la firma para los mensajes entrantes. A parte de los certificados S/MIME según el estándar X.509 (certificados de correo electrónico de clase 2), se pueden utilizar de manera opcional los certificados S/MIME de un centro de certificación oficial (actualmente SwissSign). Estos se ponen a disposición a través de Managed PKI (MPKI). Es necesario que, a parte de las condiciones estipuladas por Retarus, se acepten las condiciones adicionales del centro de certificación oficial.

Secure WebMailer

Secure WebMailer es un portal web seguro que permite a los clientes intercambiar correo electrónico cifrado con destinatarios que no utilizan S/MIME o PGP. Mediante un enlace, es posible acceder a un buzón de correo individual/personal que se crea automáticamente en Retarus Secure WebMailer para este fin. Todos los accesos están cifrados con HTTPS. El tipo de transmisión (por correo electrónico o por SMS*) de los datos de acceso personales al remitente o destinatario correspondiente de los mensajes de correo electrónico así como la configuración opcional específica para la empresa del portal Secure WebMailer se definen junto con el cliente durante el taller inicial Email Encryption Workshop.

Encrypted PDF /ZIP

Retarus ofrece la posibilidad de transmitir información confidencial en forma de documentos PDF o archivos ZIP protegidos mediante contraseña. El texto del correo electrónico, incluidos todos los archivos adjuntos, se integra en un archivo PDF o ZIP, que se cifra y se envía al destinatario. La transmisión de la contraseña para abrir el archivo PDF o ZIP y la posibilidad de adaptar la plantilla utilizada se definen junto con el cliente durante el taller inicial Email Encryption Workshop.

Initial Email Encryption workshop

El Email Encryption Workshop es un requisito previo necesario para la configuración de Retarus Email Encryption. En este taller, el cliente trabaja con Retarus para definir sus requisitos específicos para la instalación. Entre otros, pueden incluirse los contenidos siguientes:

- Introducción general a la criptografía
- Presentación de los estándares establecidos
- Evaluación de la infraestructura existente
- Análisis de los requisitos específicos del cliente y las directrices de seguridad
- Definición de flujos de trabajo y procesos, p. ej. en referencia al cifrado/firma o recogida de claves públicas
- Establecimiento del diseño y de los contenidos para las notificaciones por correo electrónico
- Definición para la utilización de Secure WebMailer (p. ej. la transmisión de datos de acceso)
- Definición para la utilización de un documento PDF cifrado (p. ej. la transmisión de la contraseña)

En función de los resultados, el cliente de cifrado específico del cliente se configura en el sistema de Retarus según los estándares S/MIME y PGP o según métodos de cifrado alternativos (Secure WebMailer/PDF o ZIP cifrado).

Ampliación para mensajes automatizados y/o generados mediante una aplicación (usuario eBusiness)

Se requiere una licencia eBusiness para el procesamiento de mensajes automatizados y/o generados mediante una aplicación procedentes de procesos automáticos fijos, aplicaciones de portales o soluciones vinculadas a procesos (por ejemplo, un módulo de firma). Para ello, a cada dirección de remitente procedente de dichas aplicaciones se le asigna una licencia especial de usuario eBusiness. En el caso de la utilización opcional de certificados S/MIME, Retarus gestiona en nombre del cliente certificados de clase 2 de la categoría “Plata”.

Data Loss Prevention

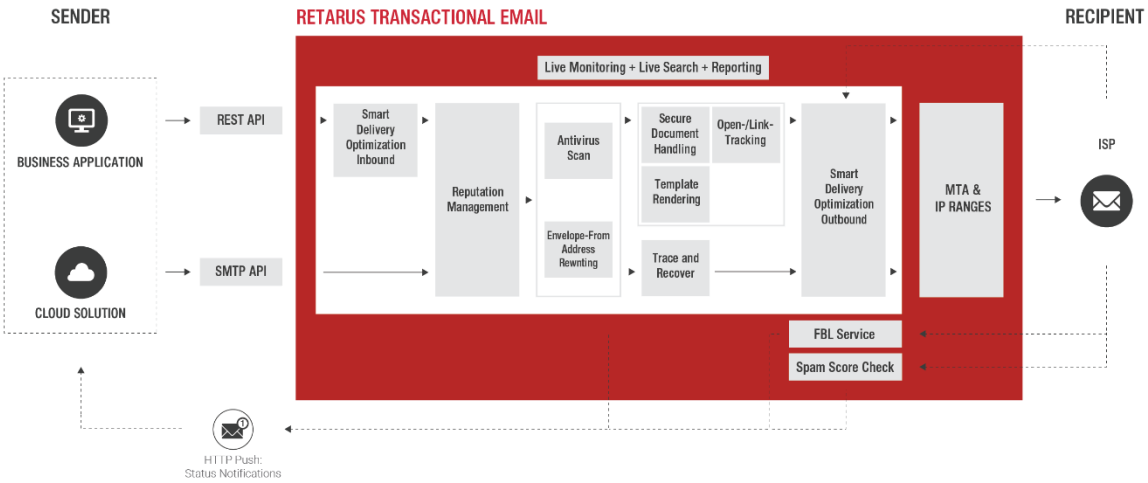
Data Loss Prevention examina mensajes de correo electrónico dirigidos a destinatarios externos por usuarios del cliente para detectar patrones definidos en el marco de la configuración, tales como números de tarjetas de crédito o números de cuentas bancarias (IBAN). Si un mensaje de correo electrónico contiene tales patrones, se impide el envío a destinatarios externos. Además, es posible informar del intento de envío a determinados empleados, p. ej. un administrador o un responsable de cumplimiento normativo. El correo electrónico en cuestión se incluirá como adjunto en la notificación. De forma opcional, se puede informar también al remitente original. El análisis en busca de tales patrones abarca el cuerpo del mensaje de correo electrónico. Además, es posible bloquear el envío de archivos adjuntos en función de extensiones de archivo (p. ej. exe, mp3, zip) y según el tipo MIME correspondiente. También es posible establecer que solo se envíen mensajes de correo electrónico a destinatarios externos si en la lista de distribución se aplica una instancia de control, p. ej. un buzón de correo funcional.

E-Mail Infrastructure

Retarus Transactional Email

Retarus Transactional Email permite enviar grandes volúmenes de correos electrónicos directamente desde la aplicación empresarial, sin sobrecargar la infraestructura de correo electrónico del cliente. Para ello, la infraestructura del cliente se conectará a Retarus Enterprise Cloud a través de interfaces estándar. Los datos se procesarán en los centros de datos de Retarus.

System Architecture Retarus 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

*Estas funcionalidades requieren el uso de direcciones IPv4.

Basic Configuration

La configuración básica del servicio incluye datos de acceso, o una IP de autenticación registrada para un punto final EPI o un servidor SMTP en un centro de datos de Retarus. La comunicación se realizará mediante una conexión segura a través de HTTPS y/o SMTP Auth Basic vía eTLS. La configuración incluye un dominio/dirección de remitente, un parámetro de trabajo por defecto, un enrutamiento IP, un registro SPF y una firma DKIM. La cuenta se activará una vez que se haya configurado completa y satisfactoriamente, y se proporcionará una descripción de la interfaz.

*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

Se asignará una dirección IP dedicada a uno o varios dominios emisores. Esto permite segregar el tráfico de correo electrónico de diferentes aplicaciones, separar las empresas matrices/filiales y dividir las regiones. Se recomienda utilizar la dedicated IP en caso de enviar un mínimo de 1.000.000 de correos electrónicos al mes. Dado que el servicio de Transactional Email se conecta generalmente a un grupo de centros de datos (Activo/Activo), el uso de la dedicated IP requiere al menos dos direcciones IP dedicadas. Una vez configuradas las direcciones IP dedicadas, Retarus proporcionará direcciones IPv4 al cliente para que las utilice durante el periodo del contrato. Estas se integrarán en el sistema de monitorización de listas negras de Retarus. Retarus puede cambiar, en cualquier momento, la dirección IP.

Enforced TLS

Durante la configuración básica del servicio, se determinará a nivel del dominio de envío si se va a utilizar un protocolo de encryption híbrido para cada correo electrónico enviado. De este modo, pretendemos establecer una conexión encriptada tan pronto como el cliente envíe correos electrónicos a través del dominio dado (enforced TLS). Si se rechaza una conexión encriptada por parte del destinatario, se cancelará el proceso de envío.

Envelope From Address Rewriting (Outbound)

Opcionalmente, Retarus ofrece Envelope From Address Rewriting para los correos electrónicos de salida con el fin de redirigir las posibles respuestas a una bandeja de entrada dedicada. La reescritura de direcciones es especialmente útil si, por ejemplo, las políticas corporativas no permiten el envío de correos electrónicos a Internet abierto a través del propio dominio de la empresa.

Account / Access Token

Una cuenta se define como una unidad de autenticación (definición de nombre de usuario/contraseña API, etc.) y está relacionada con un centro de datos específico, punto de acceso API. En cada cuenta se pueden gestionar varios dominios. También se puede gestionar el mismo dominio bajo varias cuentas.

Smart Delivery Optimization

Retarus utiliza una gestión inteligente de envío y recepción de correos electrónicos basada en el dominio de envío. La Smart Delivery Optimization adapta automáticamente el comportamiento de envío del cliente a las respuestas de cada ISP y/o ESP para mantener un alto rendimiento de los mensajes para los ISP y/o ESP. En casos excepcionales, la gestión optimizada de los envíos puede llevar a una reducción de la capacidad de procesamiento acordada.

Status Information via API Callback (Webhook)

Retarus ofrece información de estado mediante API Callback (Webhook). Se informará al cliente de los nuevos eventos creados, como el estado de la entrega, los motivos de imposibilidad de entrega o el bloqueo de correos electrónicos a destinatarios de la Suppression List, así como información sobre el seguimiento de aperturas y enlaces. Estos tipos de información de estado pueden integrarse automáticamente en los procesos y aplicaciones empresariales a través de HTTP POST para, por ejemplo, mantener los datos maestros (higiene de la base de datos) o respaldar la reputación de los dominios propios del cliente.

Retarus EAS – Live Monitoring

Retarus ofrece Live Monitoring en su Portal EAS, a través del cual se puede realizar un seguimiento de los correos electrónicos en tiempo real. Con esta solución, el cliente puede supervisar la evolución de las tendencias en los ámbitos de la entrega, los rebotes suaves/duros y los mensajes abandonados, así como iniciar las contramedidas pertinentes.

Retarus EAS – Live Search

El EAS Live Search de Retarus ofrece una visión transparente de sus correos electrónicos enviados. EAS Live Search le permite encontrar correos electrónicos de salida utilizando períodos de tiempo, ID de mensajes, remitentes y destinatarios, y recibir información detallada del estado de los últimos 45 días.

Retarus EAS – Reporting

El EAS Reporting de Retarus le ofrece un resumen transparente de los correos electrónicos enviados en los últimos 45 días, que se puede descargar como archivo CSV o Excel (XLSX).

Smart Network Data Service – Report (SNDS)

Smart Network Data Services (SNDS) le proporciona los datos que necesita para conocer su visibilidad en Microsoft y mejorarla. SNDS le permite acceder a los datos detallados de la dirección IP que utiliza, en forma de archivo CSV. Este servicio solo puede utilizarse en conexión con una dirección IP dedicada.

E-Mail Reporting (CSV)

Retarus ofrece un informe de envío en formato CSV a través del portal de servicios de administración de empresa (EAS). El cliente puede acceder a estos informes diariamente y durante un periodo de 180 días. Estos informes solo incluyen las transacciones con un estado final. Las transacciones que aún se están procesando no aparecen en la lista. Se puede acceder al informe como archivos por separado o como un único archivo comprimido (por ejemplo, como un archivo ZIP).

Atención: La elaboración de un informe CSV requiere el almacenamiento temporal de los datos para la prestación del servicio. Los datos almacenados incluyen información sobre el procesamiento de los mensajes, así como datos personales, como las direcciones de correo electrónico de los remitentes y los destinatarios, pero no datos de contenido.

Retarus Spam Score Check

La probabilidad de que los mensajes se clasifiquen como spam depende de varios factores. Un formato HTML o estructuras de tabla inusuales, un número excesivo de enlaces o una redacción dudosa en la línea de asunto o en el cuerpo del texto pueden desencadenar advertencias de spam. En este sentido, Retarus ofrece un servicio de pago de Spam Score Check. Esto le permite comprobar la probabilidad de que su correo electrónico sea clasificado como spam, antes de enviarlo. La información de Spam Score se devuelve a través de un proceso automatizado que transmite la información determinada por Retarus a través de correo electrónico a su dirección de respuesta proporcionada o a través de API Callback a su servicio web disponible. Una vez transmitida correctamente, toda la información relacionada con la transmisión se elimina y no se almacena

Open and Link Tracking (CNAME opcional)

El Open Tracking le permite determinar la tasa de apertura de los correos electrónicos, mientras que el Link Tracking le permite determinar la tasa de apertura de los enlaces contenidos en los correos electrónicos. Para este servicio, el cuerpo del correo electrónico respectivo o el enlace se modificarán de tal manera que los mensajes puedan ser evaluados. Para reducir la posibilidad de que sus correos electrónicos sean clasificados como spam, Retarus recomienda contratar el servicio CNAME. Esto permite al cliente utilizar uno de sus propios (sub)dominios. El cliente crea un A-Record del (sub)dominio en una dirección del servidor de Retarus. El cliente debe informar a los respectivos destinatarios del correo electrónico del Open y Link Tracking con una declaración de privacidad adecuada y debe obtener su consentimiento previo cuando sea necesario, de acuerdo con la legislación aplicable.

AntiVirus MultiScan

Retarus comprueba los mensajes en busca de virus durante el proceso de envío. El cliente puede determinar de antemano si solo deben comprobarse los archivos adjuntos o si también se debe comprobar el cuerpo de un correo electrónico en busca de malware. Esta comprobación se realiza con dos escáneres de virus de diferentes proveedores seleccionados por Retarus. En cuanto estos proveedores ofrecen actualizaciones o nuevas versiones, Retarus las aplica lo antes posible para la comprobación de virus. Si se encuentra un virus en un correo electrónico, Retarus elimina el correo electrónico infectado. La información sobre el estado de los correos electrónicos infectados se proporcionará al cliente a través de API Callback (Webhook).

Secure Document Handling

Los archivos adjuntos a los correos electrónicos enviados pueden encriptarse con Secure Document Handling. Para ello, los archivos adjuntos se comprimirán automáticamente en un archivo ZIP protegido por contraseña en la infraestructura de Retarus antes de su envío. Se entregará las contraseñas a los destinatarios en correos electrónicos separados. Para proporcionar la mejor protección posible a su destinatario, este servicio sólo está disponible en conexión con nuestro servicio Outbound AntiVirus MultiScan.

Trace and Recover

Esta función marca los correos electrónicos enviados a través de una conexión SMTP como mensajes de tipo Trace & Recover. Los mensajes marcados como Trace & Recover se guardan en la memoria a corto plazo durante un periodo de 45 días y pueden buscarse durante este periodo utilizando la función Retarus EAS Live Search. Para los mensajes marcados, está disponible una vista previa de los primeros 1000 caracteres. Antes de volver a enviar un mensaje, si es necesario, solo se puede editar el destinatario inicial. La función adicional Trace & Recover requiere AntiVirus MultiScan y se activa por parte de Retarus para una cuenta técnica determinada por el cliente. Trace & Recover no puede utilizarse en relación con Envelope-From Address Rewriting (salida).

Processing Capacity

Las capacidades de procesamiento se calculan utilizando la configuración básica del Transactional Email. Esto supone un tamaño de correo electrónico de 200 kilobytes e incluye Open and Link Tracking durante un período de una hora.

La garantía de capacidad de procesamiento por hora, acordada contractualmente, requiere de una distribución uniforme de las solicitudes de transmisión en Retarus. Para proporcionar la capacidad de procesamiento acordada, Retarus comprueba la distribución en intervalos de 5 minutos.

Para asegurar el rendimiento suficiente, la capacidad de procesamiento real ofrecida se incrementa un 25% sobre la capacidad de procesamiento acordada. En el caso de funciones adicionales o de correos electrónicos más grandes, el ancho de banda puede disminuir (por ejemplo, para correos electrónicos de más de 200 KB). De vez en cuando pueden producirse desviaciones en la capacidad de procesamiento. Antes de aumentar la capacidad de procesamiento, es imprescindible que Retarus revise las necesidades individuales del cliente.

Ejemplo: Capacidad de procesamiento

En el siguiente ejemplo, la capacidad de procesamiento acordada por contrato es de 150.000 correos electrónicos/hora:

- (150.000 correos electrónicos/hora) / (12 x intervalo*/hora) = 12.500 correos electrónicos/intervalo*.
- La ampliación máxima de los picos de envío del 25% puede aumentar el rendimiento de procesamiento hasta un máximo de 15.625 correos electrónicos/intervalo*.

*Un intervalo es de 5 minutos.

IP Whitelisting

El uso de la función IP Whitelisting de Retarus le permite mejorar la seguridad de sus "envíos permitidos". Usted define expresamente qué aplicaciones de su red pueden utilizar el servicio de Transactional Email y cuáles no.

Feedback Loops

Retarus se comunica con diferentes proveedores de servicios de Internet mediante un acuerdo de quejas. Los ISP implicados remitirán la información de las quejas a Retarus en forma de Feedback Loops (ARF).

Los Feedback Loops son un mecanismo proporcionado por un ISP para informar a los remitentes en cuanto sus mensajes son clasificados como no deseados. El término "no deseado" se refiere a que el destinatario del correo electrónico clasifica su mensaje como spam (por ejemplo, al hacer clic en Esto es spam, en su propia bandeja de entrada).

El feedback de la queja se lleva a cabo a través de un proceso automatizado, en el que la información de la queja transmitida se lee y envía a través de correo electrónico a su dirección de correo electrónico de respuesta o a través de API Callback a su servicio web disponible. Una vez transmitida con éxito, toda la información relacionada con la reclamación se elimina y no se almacena.

Billing

Los correos electrónicos se cobran por unidad, cada una de 200 kilobytes. A efectos de liquidación, los correos electrónicos de más de 200 kilobytes se dividirán en varias unidades.

Por ejemplo: Un correo electrónico tiene 2403 kilobytes (aproximadamente, 2,4 MB) equivale a 13 unidades de carga.

Los correos electrónicos se facturan (identificador: ID del correo electrónico) independientemente de si la transmisión se ha realizado con éxito o no (por ejemplo, si los correos electrónicos han sido bloqueados o devueltos).

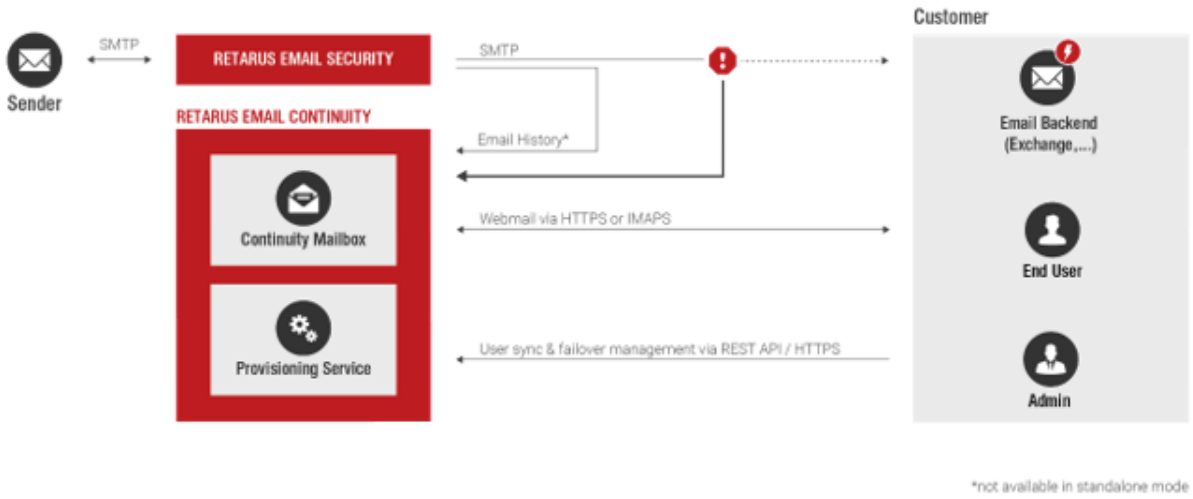
Retarus Email Continuity

Retarus Email Continuity es una plataforma de correo electrónico alternativa diseñada para la continuidad de la comunicación por correo electrónico en situaciones de catástrofe (p. ej. infiltración de malware, caída del centro de datos, periodo de inactividad en la nube). En caso necesario y si el cliente así lo solicita, la recepción y el envío de todos los correos electrónicos entrantes y salientes se redirigen a través de esta plataforma.

Funciones adicionales:

- Acceso al buzón de Email Continuity del usuario a través de webmail (HTTPS)
- Funcionalidad de directorio interno para buscar y mostrar toda la información de los contactos pertenecientes al dominio del cliente
- Acceso administrativo al servicio de continuidad vía API REST para la gestión y provisión de los buzones de usuario
- Configuración de buzones a través del servicio de Sincronización de Directorio de Retarus mediante un archivo csv
- Notificación automática para los nuevos usuarios de Continuity
- Autoservicio de gestión contraseñas a través de una landing page (mediante tokens de seguridad que los propios clientes gestionan)
- Transmisión de correos electrónicos desde el buzón de Continuity (Backsync) al entorno productivo tras restablecer el servicio
- Acceso opcional a todos los mensajes entrantes de los últimos días (historial de correo electrónico de hasta 14 días) según los dominios asignados al cliente. Para ello, se requiere un redireccionamiento de los registros MX específicos del cliente a la infraestructura de Retarus

Arquitectura del sistema Retarus Email Continuity



Retarus Predelivery Logic

Al activar el servicio “Retarus Predelivery Logic” se evalúa y modifica el comportamiento de los mensajes dentro de la infraestructura de Retarus, antes de su entrega a la infraestructura de correo del cliente.

Este comportamiento es altamente configurable y se parametriza por cliente mediante la creación de reglas individuales en el portal de EAS, compuestas por "condiciones" y "acciones". Por ejemplo, el enrutamiento y la reescritura pueden realizarse en base a cierta información de cabecera, como el remitente, el usuario o el asunto del correo electrónico.

Conexión a Retarus

Por regla general, la conexión de los sistemas del cliente a la infraestructura de Retarus tiene lugar mediante el protocolo criptográfico de Internet Transport Layer Security (TLS), a fin de garantizar la transmisión segura de los datos vía SMTP. En función de lo acordado, se puede utilizar TLS oportunista, TLS forzado o la conexión mediante una red privada virtual (VPN). Para poder realizar la conexión a través de VPN, es necesario realizar una conexión simultánea con los centros de datos de Retarus en Múnich y Frankfurt/Main (Centro de datos DE 1 y Centro de datos DE 2).

Notas

La protección contra mensajes entrantes y salientes con carácter potencialmente malicioso, además de enlaces integrados y archivos adjuntos, se basa principalmente en métodos estadísticos y de aproximación. Pese a la utilización de todas las funciones descritas, puede que se produzcan el rechazo erróneo o la clasificación errónea de mensajes, o la entrega de mensajes potencialmente maliciosos.

Asimismo, Retarus advierte de que el método de la puesta en cuarentena —dependiendo del tipo de la utilización del correo electrónico y de la configuración realizada específicamente para cada cliente— puede provocar que algunos mensajes, en particular los denominados “falsos positivos”, no se reciban o se reciban con demora, con el consiguiente posible perjuicio para el cliente.

Las siguientes opciones de servicio requieren 4x Antivirus MultiScan:

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

Salvo que se acuerde expresamente otra cosa por escrito, el uso de los servicios Retarus Email Encryption se limita a la comunicación corporativa personal. Para el procesamiento de mensajes automatizados y/o generados mediante una aplicación se requiere obligatoriamente un usuario eBusiness de Retarus Email Encryption.

Implementación, gestión de cambios y asistencia

Para solicitudes de asistencia y servicio así como para solicitudes de cambio, el cliente debe comunicar a Retarus qué personas están autorizadas oficialmente para realizar este tipo de consultas. En principio, se establecerá como primer interlocutor autorizado al interlocutor técnico del cliente responsable de la implementación de los servicios. Como administrador del cliente, este puede entonces introducir y autorizar a otras personas de contacto de asistencia adicionales en el portal EAS (Enterprise Administration Portal). Los administradores del cliente pueden modificar, ampliar o eliminar estos permisos en cualquier momento.

El cliente debe aceptar, como mínimo por escrito, los cambios realizados en el pedido del cliente en referencia a servicios o soluciones frente a incidencias (incluidas soluciones alternativas). Si el cliente no responde en el plazo de 10 días, el ticket correspondiente del cliente se cierra automáticamente después de este periodo y el cambio o la solución se considera aceptado.

Duties of Cooperation

El cliente es consciente de que el uso satisfactorio de los servicios de Retarus y la calidad de los servicios prestados dependen considerablemente de la cooperación del cliente. El cliente, por lo tanto, debe devolver rellenada la Hoja de Implementación que se le proporcionó a la conclusión del contrato, en un plazo de cinco (5) días laborables, debe cumplir escrupulosamente los deberes de cooperación establecidos en este documento y acepta que Retarus pueda tomar medidas técnicas beneficiosas para asegurar la prestación estable del servicio y proteger la reputación de ISP de las partes. Para ello, Retarus está expresamente autorizada a descartar determinados pedidos por correo electrónico, restringir el volumen o, en casos extremos, prohibir el acceso. En caso de que surjan esfuerzos o costes derivados del incumplimiento de los deberes de cooperación, correrán a cargo del cliente.

En caso de que se produzcan esfuerzos y/o costes debido al incumplimiento de los deberes de cooperación, éstos correrán a cargo del cliente.

El cliente se compromete a enviar únicamente correos electrónicos a los destinatarios que, de acuerdo con el marco legal aplicable, le hayan autorizado expresamente a hacerlo (Opt-In), o para los que exista un permiso diferente legalmente reconocido para hacerlo.

Email Design

Todo correo electrónico enviado debe incluir un pie de imprenta en el cuerpo del texto, que debe cumplir con los requisitos legales aplicables y ser fácilmente reconocible.

Además, lo siguiente se aplica al envío de correos electrónicos con contenido promocional:

- El remitente de un correo electrónico publicitario debe ser claramente visible.
- En cada correo electrónico, se debe informar al destinatario por separado acerca de que puede revocar su consentimiento para recibir correos electrónicos en cualquier momento. La revocación/cancelación de los mensajes de correo electrónico (Opt-Out/Unsubscribe) debe ser, por lo general, fácil de realizar para el destinatario; es decir, sin necesidad de introducir datos de acceso (por ejemplo, nombre de usuario o contraseña).
- El encabezado o el asunto de un correo electrónico no debe ocultar ni esconder ni el remitente ni la naturaleza comercial del mismo. Esconder u ocultar significa, en este caso, que el encabezado o la línea de asunto están diseñados intencionadamente de tal manera que el destinatario no recibe ninguna información, o simplemente una información engañosa, sobre la identidad real del remitente o la naturaleza comercial del mensaje antes de leer el contenido del mismo.

Technical Configuration

- Las direcciones del remitente deben estar registradas y formar parte de la administración del servicio. La dirección del remitente debe poder recibir correos electrónicos (registro DNS MX válido). El dominio del remitente también debe tener un DNS A-Record válido. No se permiten direcciones de remitente basadas en función (por ejemplo, abuse@ o postmaster@).
- El cliente debe eliminar inmediatamente las direcciones de correo electrónico de las respectivas listas de correo electrónico si se descubre que no existen en el momento del envío, y a más tardar si se han producido tres hard bounces. La tasa total de hard bounce por ISP no debe superar normalmente el 1,0 %. Se descartarán las direcciones de destinatarios basadas en roles (por ejemplo, postmaster@, abuse@).
- El cliente debe eliminar las direcciones de correo electrónico de las respectivas listas de correo electrónico si el destinatario clasifica el correo electrónico como spam y lo denuncia (queja) o revoca el consentimiento para recibir correos electrónicos.
- Para la dirección MAIL FROM incluida en la comunicación SMTP entre servidores de correo electrónico, debe rellenarse un SPF-From Record, lo que permite realizar una prueba SPF por

parte del destinatario. El registro SPF debe terminar en -all o ~all. En caso de que no se realicen las entradas necesarias por parte del cliente en un plazo de diez (10) días laborables, se cobrará de nuevo la comprobación por el esfuerzo.

- El cliente debe utilizar siempre el proceso DKIM (DomainKeys Identified Mail). Para cada dominio de remitente registrado para el cliente en Retarus, el cliente debe proporcionar una clave DKIM en su DNS. En caso de que no se realicen las entradas necesarias en un plazo de diez (10) días laborables, se cobrará de nuevo la comprobación por el esfuerzo.
- Todos los correos electrónicos enviados deben incluir "List-unsubscribe"- Header o "List-Help" (consulte RFC 2369). "List-unsubscribe"- Header es necesaria para los envíos de correos basados en listas y debe insertarse con un "POST HTTPS" link que incluya la función "One-click unsubscribe" (RFC 8058). El enlace proporcionado tiene que dar lugar a una cancelación directa de la suscripción con un solo clic, al menos a nivel de lista. El remitente puede enviar al usuario una confirmación después de la cancelación de la suscripción. Los correos no basados en listas deben incluir "List-Help"- Header, en lugar de "List-unsubscribe"- Header. "List-Help"- Header debe incluir al menos una dirección "mail-to" o un HTTPS link. No se permiten los HTTP links. Tanto el uso de la dirección "mailto:" como el HTTPS link deben permitir que el destinatario reciba información sobre el motivo por el que se le ha enviado el correo electrónico y por qué no es posible darse de baja en el nivel de lista.

- El uso del „list-unsubscribe-Post“-Header requiere una dirección URL válida que pueda recibir y procesar dichas solicitudes POST.
  Por ejemplo:

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

- Los enlaces proporcionados deben desencadenar una suscripción simplificada en 1 clic al menos a nivel de la lista. El cliente también se compromete a enviar al destinatario un correo electrónico en el que confirme que se ha dado de baja. Se pueden hacer excepciones a esta obligación si no es posible darse de baja de los correos electrónicos en el sentido antes mencionado debido al diseño del servicio y al envío asociado de correos electrónicos automatizados.
- El Cliente debe configurar una dirección de email de abuso para la notificación del abuso de las direcciones de email para los destinatarios de los emails y monitorizarla. La dirección de email abusiva puede configurarse, por ejemplo, como abuse@domain.
- El envío de emails al servicio de Retarus Transactional Email debe realizarse a través de Transport Layer Security (TLS - opportunistic/enforced) del cliente, según el estado actual de la técnica. Retarus utiliza para el envío de emails al destinatario Transport Layer Security (TLS) mientras utiliza direcciones IP de CSA.
- Retarus cuenta con la certificación CSA (Certified Senders Alliance). Las obligaciones de cooperación aquí descritas reflejan los requisitos actuales de la CSA. La CSA puede adaptar sus requisitos en cualquier momento. Por lo tanto, el cliente se compromete a cumplir con dichos cambios. Retarus informará a los clientes de dichos cambios.