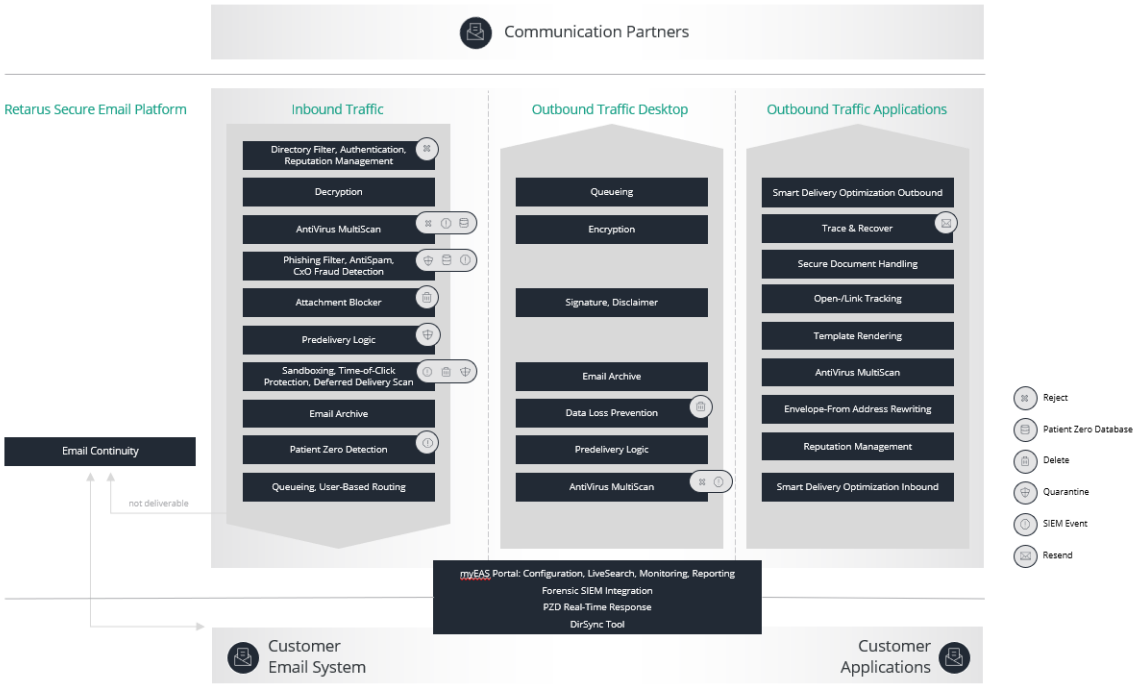
Service Description and Duties of Cooperation
Retarus Secure Email Platform

The **Retarus Secure Email Platform** combines comprehensive security (Advanced Threat Protection, a patented Postdelivery Protection, Sandboxing), enhanced email routing via the Predelivery Logic, with Email Archiving, Email Encryption and Email Continuity. Additionally, existing business applications can be connected to the platform via the Retarus Transactional Email modules.

The range of services are structured into the following main product categories: **Email Cloud Gateway**, **Email Security**, **Email Compliance** and **Email Infrastructure**.

Content

System Architecture Retarus Secure Email Platform



Email Cloud Gateway

The **Retarus Email Cloud Gateway** offers foundational functionalities for managing and securing the SMTP message traffic. It can be used as a stand-alone service, but may also be expanded using additional modules of the Retarus Secure Email Platform.

The Email Cloud Gateway includes the following functionalities:

Directory Filter / Reputation Management

The Director Filter rejects those emails in a RFC-compliant way ('reject method') addressed to recipients not configured in the Retarus Enterprise Administration Services Portal (EAS Portal). This can be configured and updated either manually by the customer through the EAS Portal itself, or automatically through Directory-Synchronization in a format specified by Retarus with the customer's address books and directories.

The reputation of senders of incoming emails is checked via the Inbound Reputation Management which supplements the Directory Filter. A sender's authorization is validated via the SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) mechanisms. In the event of failed validation of classified emails, such emails are handled in accordance with the Customer configuration in the EAS portal or - if activated by Customer - further processed pursuant to the DMARC policy specification (Domain-based Message Authentication, Reporting & Conformance) of the domain owner (sender) (actions: None, Quarantine, Reject).

Note: The use of DMARC requires routing to a dedicated MX record of Retarus.

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.

DHA Protection

Directory Harvest Attack (DHA) protection for the email domain(s) selected by the domain owner. Messages to invalid recipients within the domain concerned will be rejected. The receipt of additional messages to invalid recipients will be restricted by throttling the identified sender of these messages.

Backscatter Protection

Protection from misuse of bounce messages automatically generated for sending (Backscatter).

Backscatter is unauthorized use of another person's valid email address for spam campaigns. It may be the case that the receiving email server of the recipients receives a large number of delivery status notifications (e. g. if the receiving address does not exist) at the valid email address of the person that was used as the sender without their knowledge. Emails are not delivered to the actual sender.

Thanks to Backscatter Protection, an increased number of these automatically-generated messages will be identified and filtered out, and their delivery will be prevented using isolation of the recipient concerned in personal quarantine. In personal quarantine, these messages will be marked as NDR Spam.

Email Back-up / Queuing

In case of undeliverability of the messages intended for the customer, Retarus will store the respective incoming messages for a maximum of 96 hours. Should the undeliverability not be able to be resolved, the sender of the message will receive a notice of undeliverability via email. Retarus will attempt delivery in regular short intervals throughout this span of 96 hours. Should undeliverability end within this time span, the incoming messages will be forwarded by Retarus in batches.

Large Email Handling

Retarus Large Email Handling allows you to reliably block emails above a defined size, or alternatively, depending on your settings, to store them securely in Retarus' own datacenters. In the latter case, the recipient is notified by email and may release affected messages individually. The recipient will be informed such an email, should this have been configured. The user may download this email using an HTTP link and simplified authentication (OneClick token login).

User-based Routing

As part of user-based Routing, Retarus delivers emails for previously-defined recipients within a domain to a certain destination server.

Email Signature / Disclaimer

The customer has the opportunity of storing signatures or disclaimers in the Enterprise Administration Services Portal (EAS Portal). Retarus then attaches the signatures or disclaimers created via the EAS Portal to the customer's outbound emails. When using placeholders, these will be replaced with data from Directory Synchronization.

Email Live Search

Email Live Search provides detailed results on the status of individual emails in real time. This search function makes it easier to find emails, simplifies the analysis of delivery delays, and supports IT forensics. For example, the help desk can release emails marked as graymail to users from within user guidance.

Access Management

A customer may assign access permissions for individual administrators according to the customer's requirements via the Retarus Enterprise Administration Services Portal (EAS Portal), e. g. different access permissions for certain countries, branches, domains or departments.

Email Security

Retarus Email Security protects complex email infrastructures from malware like viruses, spam, phishing emails, ransomware and other digital threats. The multi-level filtering methods and data sources are constantly kept up to date and optimized. Data processing takes place in Retarus' own data centers pursuant to the data protection rules currently in force.

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 4-stage

Like AntiVirus Multiscan 2-stage, checking for viruses takes place, but using virus scanners by four different providers.

External Sender Visibility Enhancement

External Sender Visibility Enhancement marks incoming messages that use a sender domain assigned to the customer for sending. For sender validation, the header field 'MIME-FROM' is used. Incoming messages will be marked using pre-defined Unicode icons (symbols) within the Retarus infrastructure, before being transmitted to the customer's infrastructure. Marking takes place in the 'friendly name' sender field.

AntiSpam Management and Phishing Filter (Inbound)

The messages received by Retarus and meant for the customer, will be checked using the respective spam filter utilized by Retarus, assigned a SPAM probability score and identified as 'potential spam' using the customer-specific limits. Those messages identified as 'potential spam' will not be delivered directly but rather treated in quarantine management according to the configuration. Alternatively, messages recognized as SPAM can be marked accordingly and delivered if configured by the customer wishes ('tag and deliver'). Retarus utilizes different filter, pattern, recognition procedures and technologies to achieve this. The phishing filter checks links in incoming emails against special sources for phishing URLs. Recognition and further processing of the messages quarantined are to be carried out by the customer and their defined users.

AntiSpam Management and Phishing Filter (Outbound)

Similar to Retarus AntiSpam Management and Phishing Filter (Inbound), the Outbound counterpart employs the renowned spam filter technology utilized by Retarus. Each outgoing email is assigned a SPAM probability score, and those surpassing a configurable threshold (default set at 60%) are subject to different disposition options based on your configuration preferences. The available choices include rejection, temporary failure (tempfail), or silent discarding, allowing you to tailor the response to align with your specific security policies. The configuration flexibility extends to all hierarchy levels, enabling you to fine-tune settings at the customer, domain, profile, and user levels. To activate the feature, please reach out to the Retarus Support team.

Attachment Blocker

Delivery of certain email attachments may be prohibited according to the customer's configurations. Attachments to be blocked can be selected using data type extensions (e. g. exe, mp3, zip) as well as using the respective MIME types. The file attached to an incoming email will either be deleted and only the email body will be delivered to the recipient, or a copy of the original email including the attachment is sent to a pre-defined mailbox (e. g. administrator). Recipients can be informed about deleted attachments using configurable notifications.

Outbound Recipient Restriction

By default, outgoing emails processed by Retarus may have up to 600 recipient addresses. If an email exceeds this threshold, Retarus rejects it for the exceeding recipients, and notification depends on your email server's configuration. Our Outbound Recipient Restriction feature empowers you to set a custom maximum number of recipients (0-600) for outbound emails. Exceeding the configured limit can trigger rejection, temporary failure, or silent discard based on your preferences. This capability is aimed at limiting recipients, preventing identity exposure, and facilitating efficient administration. The feature may be configured on all hierarchy levels (customer, domain, profile, user). To activate this feature, assistance by the Retarus Support team is initially required.

Outbound Size Restriction

By default, outgoing emails processed by Retarus may have a size up to 250 MB (256000 kB). The “Outbound Size Restriction” feature allows you to restrict the size of outgoing (Outbound) emails even further, if required. Exceeding the configured limit can trigger rejection, temporary failure, or silent discard based on your preferences. The feature may be configured on all hierarchy levels (customer, domain, profile, user). To activate this feature, assistance by the Retarus Support team is initially required.

Deferred Delivery Scan

As part of Deferred Delivery Scan (DDS), specific file attachments are further analyzed using additional re-scan procedures. Using these additional scans with more current signatures, delivery of harmful content which have not been identified during the first scanning, can be prevented at a higher rate. If a virus is found in an email, Retarus deletes the infected email and sends notifications according to the configuration in quarantine management. As DDS leads to delayed delivery of incoming email, potentially-agreed service levels in regard to delivery times may not apply.

Time-of-Click Protection

Links included in emails are automatically re-written (URL Rewriting). If the recipient clicks on the respective links, these will be checked for target addresses, suspected of being involved in phishing. Should the target site not be recognized as phishing, the user will be forwarded directly. Should the target site be a phishing site, a security warning will be displayed. After termination of the service, the respective links may no longer be immediately reachable.

CxO Fraud Detection

CxO Fraud Detection uses algorithms identifying 'From Spoofing' and 'Domain Spoofing', and recognizing fake recipient addresses (e. g. high-ranking superior within company). Messages classified as CxO Fraud will be treated in quarantine management according to the configuration.

Sandboxing

During Sandboxing, specific file attachments are further analyzed. Attachments including potentially harmful content will be executed by a virtual machine and checked for unusual behavior. For these checks, a specialized third-party provider's Sandbox solutions is used. In the case of an infection with harmful content being identified, the respective messages will be treated in quarantine management according to the configuration. Given that Sandboxing etc. may lead to delayed delivery of incoming emails, depending i. a. on file size, file type and number of file attachments, potentially-agreed service levels regarding delivery times may not apply.

Patient Zero Detection®

Patient Zero Detection® creates a digital fingerprint ('Hash') of all file attachments and links during receipt by the email addresses directed to the customer's recipients. Should the virus scanners employed by Retarus detect harmful content in attachments or links at a later time, also recipients of delivered and potentially harmful messages can be identified early on. The customer's administrators and the recipient of the messages, if instructed to do so, will be informed about this immediately. The customer, thus, has the opportunity to take measures to remove the harmful code from their infrastructure or prevent spreading of the harmful code.

Patient Zero Detection® Real-Time Response

Thanks to Patient Zero Detection® Real-Time Response, Retarus can offer software that the customer can operate within their own infrastructure. This software automatically processes messages identified as harmful by Patient Zero Detection® after delivery to the recipient's mailbox. These messages can, then, be deleted from the recipient's mailbox automatically. In order to operate Patient Zero Detection® Real-time Response, using 'Retarus Forensic SIEM Integration' as well as a connection to Microsoft Exchange on the customer's side are necessary. For Patient Zero Detection® Real-time Response, separate terms of use apply, which the customer has to consider and adhere to in the case of installing and using the software. These terms of use can be found in the EAS Portal as well as online.

Quarantine Management

As part of Quarantine Management, the customer, and, if requested by the customer, their individual users, can request delivery of an email security report (Digest) at customizable points in time. The Digest, depending on the requested options, includes a combined overview over emails, which were quarantined or deleted by Retarus based on Graymail (e. g. newsletters), viruses, spam, phishing, Sandboxing, CxO Fraud etc. within the defined time period. Quarantined messages can be accessed by the customer by clicking on the respective entry in the digest within the defined time period (for a maximum of 30 days). Should the customer have so decided, the individual recipients can access their quarantine online and create their own settings. The customer's administrators can configure quarantine settings across the system using the Enterprise Administration Services Portal (EAS Portal).

Forensic SIEM Integration

As part of Forensic SIEM Integration, Retarus provides an interface that the customer can use to request information about events and results (Event, and Log), resulting from in- and outbound messaged within the Retarus Email Security. This can be included into an existing SIEM tool as an additional data source. Events provided for the customer depend on the booked options and are available for:

- AntiVirus Multiscan (inbound and outbound)
- Sandboxing
- CxO Fraud Detection
- Patient Zero Detection®
- Outbound emails, in general
- Inbound emails, in general

Email Compliance

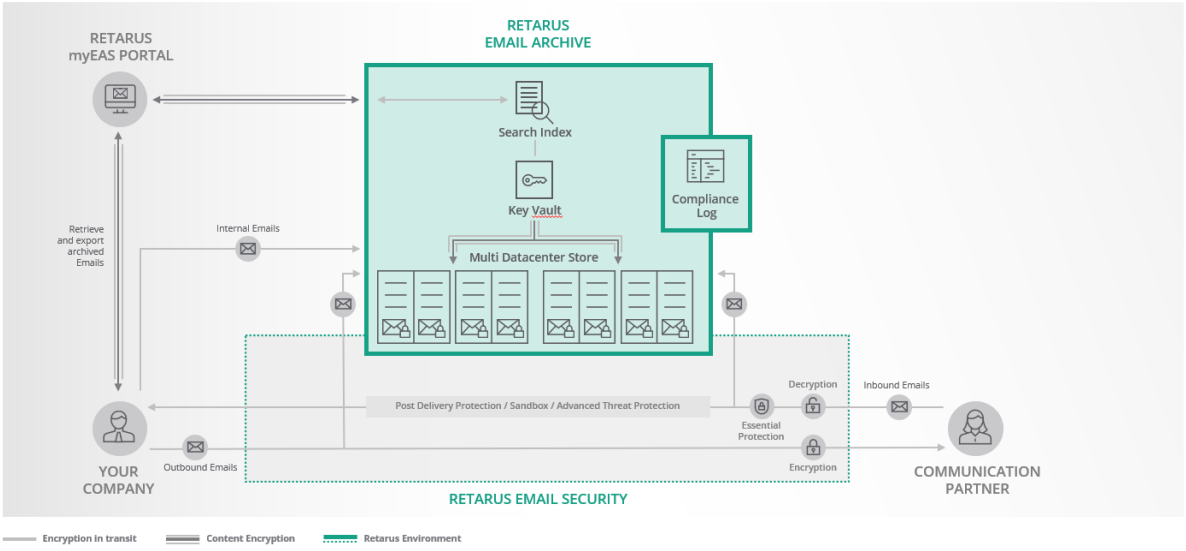
Retarus Email Archive

The **Retarus Email Archive** stores incoming and outgoing email communication – automatically, reliably and for the long term. If required, internal email communication can also be stored in the Retarus Email Archive.

Messages handed over to the Retarus Email Archive are uneditable, protected from unauthorized access and retrievable. These messages are stored for the term of the agreement, for a maximum of ten years, and will be deleted at the end of the agreed duration in compliance with the law, unless agreed otherwise. During the archiving period, archived emails can be found and re-delivered easily by the customer, using various filtering options. Should the customer wish to export the entire archive before the end of the agreed archiving period and the deletion of the emails, this is to be requested by the customer before the end of the term.

Administrator access to the email archive is based on the dual-control principle. Archived emails and attachments can be found quickly using powerful search functionalities, which can be restricted granularly, if necessary, e.g., in the case of data protection requirements.

A complete access protocol will be created automatically.



Functionalities:

- Reliable long-term storage of all incoming and outgoing emails
- Uneditable, secure data storage based on hybrid encryption
- Providing tracking information via EAS Live Search
- Access protocol created automatically
- Support in meeting regulatory requirements
- Messages retrievable incl. attachments
- Access based on dual-control principle via the web-based Retarus administrative portal
- Powerful search functionality with configuration option for data-protection compliance: Finding emails based on sender, recipient or attachment file format; configurable storage of respective (meta) data for search by subject, full text or attachment name

Options upon request

- Archiving of internal email communication via Journaling (Microsoft Exchange or M365 Exchange Online)
- Secure and convenient access for customer's administrators via Single Sign-on
- Importing emails from other archiving systems (ideally in eml format)
- Exporting archived emails to external data storage
- Using customer's own (public) keys (private keys remain with customer)

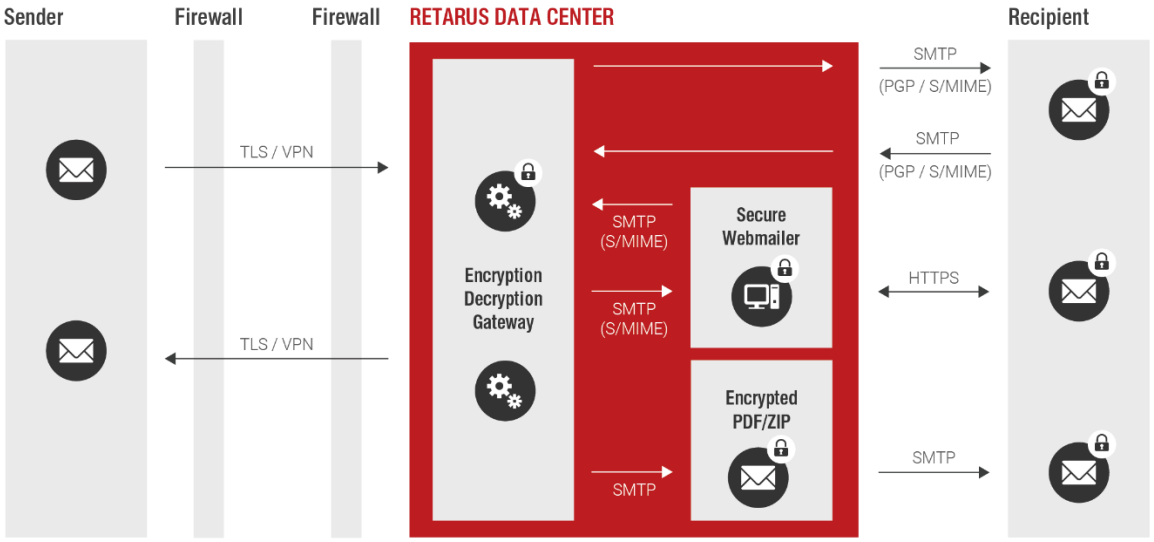
Retarus Email Encryption

Retarus Email Encryption supports the customer to maintain integrity, authenticity and confidentiality of email messages. In order to do so, emails are either encrypted in the Retarus System including their attachment via pre-defined rules or on a user-specific basis, and/or signed on an on-demand basis before sending them to the recipients. A requested check for viruses is carried out before encryption for outgoing emails and after decryption for incoming emails.

Further functionalities:

- Adopting existing Public Key Infrastructures (PKIs)
- Further use of existing and valid S/MIME certificates
- Support of Open PGP, PGP and S/MIME standards
- Integration of customer's own encryption policies
- Provision of Microsoft Outlook Add-ins for controlling user actions for encryption and/or signature of messages
- Provision of alternative encrypted ways of communicating via the Retarus Secure WebMailer or sending of encrypted PDF or ZIP files
- Optional integration of an official Trust Center (currently SwissSign) for creating S/MIME certificates according to X.509 standard
- Automated user synchronization for creating and renewing certificates (upon request)

System Architecture of Retarus Email Encryption



Initial Email Encryption workshop

The initial Email Encryption workshop is a necessary requirement for configuring Retarus Email Encryption. In this workshop, the customer, together with Retarus, will define customer-specific requirements for setup. Topics may include:

- Introduction to cryptography,
- Presentation of established standard,
- Taking stock of existing infrastructure,
- Analysis of customer-specific requirements and security policies,
- Definition of workflows and processes, e. g. pertaining to encryption/signature or collecting public keys,
- Definition of layouts and contents for email notifications,
- Definition for using the Secure WebMailer (e. g. transmission of access data),
- Definition for using an encrypted PDF document (e. g. transmission of password).

Based on the results of this workshop, the Retarus sets up customer-specific encryption mandates in the Retarus system, based on the S/MIME and PGP standards or alternative encryption methods (Secure WebMailer / encrypted PDF or ZIP).

User Synchronization for Encryption (USE)

The User Synchronization for Encryption (USE) is a solution that simplifies the management of encryption users, groups and their associated S/MIME or PGP keys. With the focus on improving user experience and reducing the manual intervention, USE automates the renewal, verification and revocation process of certificates and keys by monitoring the expiration dates and initiating the necessary action.

- Capable of securely importing encryption users and assigning them to predefined groups.
- Manages policies based on customer requirements and user groups.

- Automates creation/revocation and synchronization of S/MIME (SwissSign).
- Distinguishes between personal and team certificates to avoid disruptions.
- Features fully automated recertification or semi-automated recertification.
- Creates/deletes PGP keys and synchronizes corresponding private keys for each user.
- Allows import of keys/certificates separately created/bought by customers.
- Rule notation for administering customer-specific encryption policies in a human-readable way.
- Capable of generating sync reports and S/MIME transactional reports for compliance and auditing.
- Reports can be received via email or stored on the SFTP share for collection.

Digital Signature / Certificates

Using Retarus Email Encryption, outbound emails can be signed on demand or automatically pursuant to the rules, using PGP keys or S/MIME certificates. For inbound emails, the user can easily see the result of the signature check thanks to transparent information. In addition to S/MIME certificates according to standard X.509 (email certificates of class 2), optional S/MIME certificates of a trust center (currently SwissSign) can be used. Such certificates are provided via the Managed PKI (MPKI). As well as the Retarus terms and conditions, customers are also required to accept the trust center's terms and conditions.

Secure Webmailer

Secure Webmailer is a secure web portal that customers can use to exchange encrypted emails with communication partners who neither use S/MIME nor PGP. To this end, a personal mailbox automatically created in the Retarus Secure WebMailer can be accessed via a link. All access is HTTPS-encrypted. Transmitting personal access data to the respective communication partner as well as optional enterprise-specific design of the Secure WebMailer and the notifications intended for the respective email sender and recipient are defined together with the customer as part of the initial Email Encryption workshop.

Encrypted PDF /ZIP

Retarus offers the opportunity of transmitting confidential information as a password-secured PDF document or a password-secured ZIP file. When doing so, the email text body including all attachments is integrated into a PDF or ZIP file, which is encrypted and then forwarded to the recipient. The transmission of the password for opening the PDF document or ZIP file as well as an optional adaptation of the template used will be taken care of together with the customer in the initial Email Encryption workshop.

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

Processing of machine- and/or application-generated messages from fixed automatisms, portal applications or process-linked solutions (e. g. a signature module) takes place via a so-called eBusiness licence). Doing this, each sender address of such an application is assigned to an individual eBusiness user licence. When optionally using S/MIME certificates, Retarus manages class 2 certificates of the 'silver' category on the customer's behalf.

Data Loss Prevention

Data Loss Prevention checks emails from senders on the customer's side to external recipients for patterns defined as part of the configuration, e. g. credit card number or bank account numbers (IBAN). Should an email contain such a pattern, transmission to external recipients is prohibited. Additionally, certain members of staff, e. g. an administrator or a compliance officer, may be informed about such an attempt of sending. The email in question will be attached to the notification. Optionally, the original sender may also be informed. Checking for such patterns includes the email body. Furthermore, sending attachments can be prohibited using file extensions (e. g. exe, mp3, zip) as well as the respective MIME

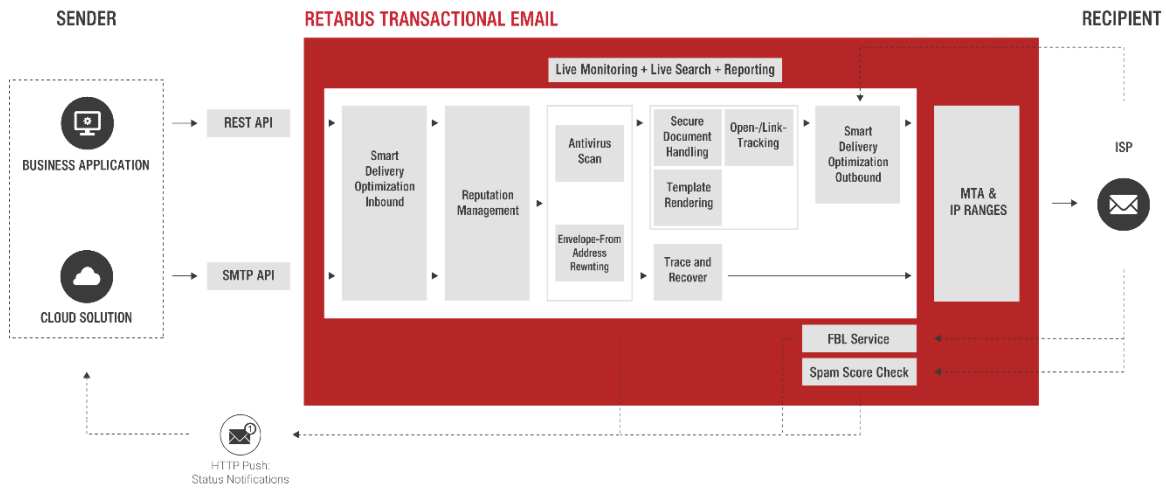
type. Additionally, the customer can specify that emails are only sent to external recipients if a supervisory body, e. g. a functional mailbox, is part of the mailing list.

Email Infrastructure

Retarus Transactional Email

Using **Retarus Transactional Email**, large volumes of emails can be sent from business application directly, without burdening the customer's own email infrastructure. To this end, the customer's infrastructure will be connected to the Retarus Enterprise Cloud via standard interfaces. The data is processed in Retarus' own data centers.

System Architecture of Retarus Transactional Email



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

*These functionalities require using IPv4 addresses.

Basic Configuration

The basic configuration includes access data, or a registered authentication IP for an API end point or an SMTP server in a Retarus data center. Communication will take place using a secure connection via HTTPS and/or SMTP Auth Basic via eTLS. The setup includes a sender domain/IPv6 address, default job parameter, IP Routing, SPF record and DKIM signature. The account will be activated after complete setup of the requested packages and an interface description will be provided.

*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

One or more sender addresses will be allocated a dedicated IP address. By doing so, e. g. the email traffic from various applications, parents or subsidiaries can be differentiated. Using Dedicated IP is recommended for volumes of ≥ 1,000,000 emails monthly. Given that the Transactional Email Service is generally connected to a group of data centers (active/active), the use of Dedicated IP requires at least two dedicated IP addresses. Once the dedicated IP addresses are set up, Retarus will provide IPv4 addresses for Customer’s use for the duration of the contract term. These will be integrated into Retarus' blacklist monitoring system. Retarus reserves the right to exchange the IP address at any time.

Enforced TLS

During the basic configuration of the Service, it will be determined at the sending domain level, whether a hybrid encryption protocol is to be used for every email sent. Thus, the system attempts to establish an encrypted connection as soon as the Customer sends emails via the specified domain (enforced TLS). If an encrypted connection is declined on the recipient's side, the sending process will be cancelled.

Envelope From Address Rewriting

Optionally, Retarus offers Envelope From Address Rewriting for outbound emails in order to re-direct potential replies to a dedicated inbox. Rewriting of addresses is especially useful if, for example, corporate policies do not allow emails to be sent into the open Internet via the company's own domain.

Account / Access Token

An account is defined as an authentication unit (definition of API username/password, etc.) and is related to a specific data center, API access point. Multiple domains can be managed under each account. You can also manage the same domain under multiple accounts.

Smart Delivery Optimization

Retarus uses smart send and receive control of emails based on the sending addresses. Smart Delivery Optimization automatically adapts the Customer's sending behavior to the responses of individual ISPs and/or ESPs in order to keep the message throughput high for ISPs and/or ESPs. In exceptional cases, optimized transmission management can lead to a reduction in the agreed processing capacity.

Status Information via API Callback (Webhook)

Retarus offers status information via API Callback (Webhook). The customer will be informed of newly-created events, e.g., delivery status, reasons for undeliverability, blocking of emails to recipients in the Suppression List, and information about open and link tracking. These status information types can be automatically integrated into business processes and applications via HTTP POST, e.g., to maintain master data (database hygiene) or support the reputation of the customer’s own domains.

Retarus EAS – Live Monitoring

Retarus offers Live Monitoring in its EAS Portal, through which emails can be tracked in real time. Using this solution, the customer can recognize trend developments in the areas of delivery, soft/hard bounces and dropped messages, and initiate counter measures accordingly.

Retarus EAS – Live Search

Retarus EAS Live Search provides a transparent overview over sent emails. EAS Live Search enables Customer to search for outbound emails based on time periods, message IDs, senders and recipients, and to obtain detailed status information of the past 45 days.

Retarus EAS – Reporting

Retarus EAS Reporting provides a transparent overview of emails sent in the past 45 days, downloadable as CSV or Excel (XLSX) file.

Smart Network Data Service – Report (SNDS)

Smart Network Data Services (SNDS) provide the data needed to understand and improve Customer’s reputation at Microsoft. SNDS gives Customer access to detailed data (in the form of a CSV file) of the IP address used. This service can only be used in connection with a dedicated IP address.

Email Reporting (CSV)

Via the EAS, Retarus provides a daily transmission report in CSV format available for retrieval by Customer for a period of 180 days. These reports only include transactions with a final status. Transactions that are still being processed are not listed. The report can be accessed as several file parts or compressed (e.g. as a ZIP file).

Please note: Creating a CSV report requires temporary data storage for service provision purposes. The data stored includes information about message processing as well as personal data, such as senders' and recipients' email addresses, but no content data.

Retarus Spam Score Check

The likelihood of messages being categorized as spam depends on several factors. Unusual HTML formatting or table structures, excessive numbers of links or dubious wording used in the subject line or the text body can trigger spam warnings. The purchase of the optional Retarus Spam Score Check service enables Customer to check their emails for the probability of being categorized as spam – before sending. The SpamScore is returned via an automated process which transmits the determined information from Retarus via email to the reply-to address provided by Customer, or via API Callback to Customer's available web service. After transmission, all related information is deleted; no data will be stored.

Open and Link Tracking (optional CNAME)

Open Tracking allows Customer to determine the opening rate of emails, while Link Tracking enables Customer to track the opening rate of links contained in emails. The respective email body and/or the link will be modified so that the messages can be analyzed. To reduce the potential of as spam classification, Retarus recommends the purchase of the CNAME option, which allows Customer to use one of their own (sub)domains. In this case, the Customer associates an A Record of the respective (sub)domain with a Retarus server address.

AntiVirus Multiscan

Retarus checks messages for viruses during the sending process, using two virus scanners from different Retarus providers. Retarus will use provider updates or new releases as made available. The Customer can pre-define, whether only attachments and/or the body of an email are to be checked for malware. If a virus is detected, Retarus deletes the infected email. Status information for infected emails will be provided to the Customer via API Callback (Webhook).

Secure Document Handling

File attachments in emails to be sent can be encrypted with Secure Document Handling. Attachments will be automatically packed in a password-protected ZIP archive in the Retarus System before sending. The passwords will be provided to the recipients in separate emails. In order to provide the highest possible protection to recipients, this feature is only available in connection with Retarus' Outbound AntiVirus MultiScan service.

Trace & Recover

This feature marks emails sent via an SMTP connection as Trace & Recover messages. Messages marked for Trace & Recover are stored in short-term storage for a period of 45 days and can be found during this period using the Retarus EAS Live Search function. For marked messages, a preview of the first 1,000 characters is available. Before a message can be re-sent, if required, only the initial recipient can be edited.

The additional Trace & Recover function requires AntiVirus MultiScan and is activated by Retarus for a technical account to be determined by the customer. Trace & Recover cannot be used in connection with Envelope-From Address Rewriting (outbound).

Processing Capacity

Processing capacities are calculated in accordance with the basic configuration of Transactional Email assuming an email size of 200 kilobytes and including Open and Link Tracking for a one-hour period.

A contractually agreed processing capacity on an hourly basis requires an even distribution of transmission requests at Retarus over the course of an hour by the Customer as outlined in the example below. To provide the agreed throughput, Retarus checks the distribution in 5-minute intervals.

Due to possible send peaks, the actual processing capacity may be 1.25 times the agreed processing capacity. In the case of additional features or larger emails, the bandwidth may decrease (e. g. for emails larger than 200 KB). Deviations in processing capacity may occur from time to time. A review of Customer's individual requirements by Retarus is essential before processing capacity can be increased.

Example: Processing Capacity

In the following example, the contractually-agreed processing capacity is 150,000 emails/hour:

- (150,000 emails/hour) / (12 x interval*/hour) = 12,500 emails/interval*
- The maximum extension for send peaks of 25% can increase the thoughput to a maximum of 15,625 emails/interval*.

*One interval is 5 minutes.

IP-Whitelisting

With the Retarus IP-Whitelisting feature Customers can improve their 'permitted transmission' security. Customers expressly define which applications in their network are allowed to use the Transactional Email Service and which are not.

Feedback Loops

Retarus communicates with different Internet service providers ("ISP")via complaint agreements. Complaint information will be reported back to Retarus by these ISPs in the form of feedback loops (ARF).

Feedback loops are a mechanism provided by the ISP to inform senders (here Retarus) when their messages are classified as unwanted. 'Unwanted' refers to your message being classified as spam by the email recipient (e.g. click on 'This is spam' in their own inbox).

The complaint feedback is carried out in an automated process, in which the complaint information transmitted is read out and fed back by Retarus – via email to Customer's reply-to email address or via API Callback to Customer's available web service. After transmission, all related information is deleted; no data will be stored.

Billing

Emails are charged per unit, with one unit being 200 kilobytes. Emails exceeding 200 kilobytes will be split into several units for billing purposes.

Example: An email is 2,403 kilobytes (approx. 2.4 MB): this equals 13 billing units.

Emails are invoiced (identifier: email ID) regardless of successful delivery (e.g. if blocked or bounced).

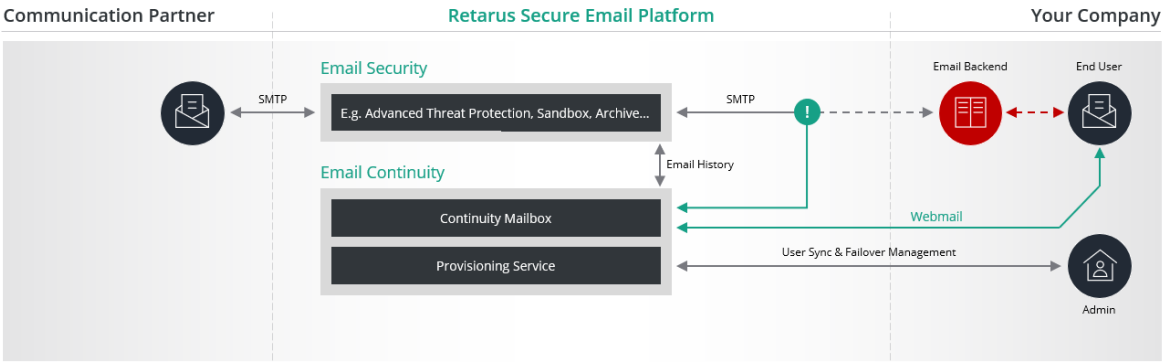
Retarus Email Continuity

Retarus Email Continuity is an alternative email platform for ensuring email communication in disaster scenarios (e. g. malware infiltration, data center malfunction, cloud downtime). If required by the client, the receipt and sending of in- and outbound emails are routed via this platform.

Further functionalities:

- End-user access to the email continuity mailbox via webmail (HTTPS)
- Internal directory functionality for displaying and finding all transmitted contact information within the customer domain concerned.
- Administrative access to the Continuity service via REST API for managing continuity mailbox users.
- Mailbox setup via the Retarus Directory-Synchronization using a csv file
- Automatic notification of newly-added Continuity users
- Password self-service via a landing page (via security tokens that the customers manages)
- Back-transmissability of emails from the email continuity mailbox (Backsync) to the productive environment.
- Optional access to all inbound messages of the last few days (email history of up to 14 days) according to the domains assigned to the customer. For this, a reference to the customer's specific MX records to the Retarus infrastructure are required

System Architecture Retarus Email Continuity



Retarus Predelivery Logic

Using the Retarus Predelivery Logic, the processing of messages within the Retarus infrastructure is influenced, before delivery to the customer's infrastructure. Customer-specific

The customer configuration takes place via creating individual rules in the EAS portal, made of 'conditions' and 'actions'. For example, Routing and rewriting can be done based on certain header information such as sender, user or email subject.

Connection to Retarus

The connection of the customer's systems to the Retarus infrastructure normally takes place via the internet encryption protocol Transport Layer Security (TLS) in order to maintain secure transmission of the data via SMTP. Based on the assignment, connection via opportunistic TLS or enforced TLS is possible.

Email Security Services can, optionally, be connected via a Virtual Private Network (VPN). A simultaneous connection to Retarus data centers in Munich and Frankfurt am Main (RZ DE 1 and RZ DE 2) is required for a VPN connection.

Please note:

The protection from inbound or outbound messages of a potentially-harmful nature next to embedded links and attachments is based, predominantly, on statistical and approximation methods. Despite using all performance features described, there may be erroneously rejected, incorrectly marked or potentially-harmful messages that are delivered.

Additionally, Retarus would like to point out that quarantining, depending on the type and way of email usage and customer-specific settings, can potentially lead to messages, especially so-called 'false positives' not being delivered or being delivered late and may lead to disadvantages for the client.

Following service options require AntiVirus Multiscan 4-stage:

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

As far as not explicitly agreed in writing, using Retarus Email Encryption is limited to personally-generated company communication. Processing of machine- and/or application-generated messages strictly requires a Retarus Email Encryption eBusiness user.

Implementing, change management and support

Implementation begins after award of contract and delivery of the completely and correctly filled-in setup sheets by the customer.

For support and service questions, as well as change requests, the customer must inform Retarus of the circle of authorized persons who can officially ask such questions. The customer's technical contact for implementation of the service is generally established as the first authorized point of contact in such matters. As the customer administrator, he can then enter further support contacts in the Enterprise Administration Portal and thereby authorize them. Customer administrators can change, expand, or delete these authorizations at any time.

Changes to the service and solutions for incidents (including workarounds) implemented in the customer order have to be accepted by the customer at least in text format. If the customer has not replied within 10 days, the relevant customer ticket will be automatically closed after this period has ended and the change/solution will be considered accepted.

Duties of Cooperation

The customer is aware that successful use of Retarus services and the quality of the services provided depends considerably on the customer's cooperation. The customer, thus, will return the filled-in Implementation Sheet, which was provided to them upon conclusion of the contract, within five (5) working days, will adhere especially to the duties of cooperation set out in this document and agrees that Retarus may take technical measures beneficial for securing stable service provision and the parties' ISP reputation. To this end, Retarus is expressly permitted to discard specific email orders, restrict the volume or, in extreme cases, ban access. Should efforts and/or cost arise from non-compliance with duties of cooperation, these are to be covered by the customer.

The Customer undertakes to solely send emails to recipients who, according to the applicable regulatory and legal framework, have given their express consent (opt-in) to receive such emails, unless other legally recognized permission exists. Customer shall comply with notification requirements, privacy statements e.g. in the context of Open or Link Tracking - or otherwise, if applicable – in accordance with applicable laws and regulations.

Email Design

Each email sent must contain easily identifiable legal details that comply with the applicable statutory requirements.

Additionally, the following applies to emails with advertising/promotional/marketing content:

- The initiator of such emails must be clearly recognizable.
- In each email, the recipient must be made aware of the option to unsubscribe or opt out from receiving emails at any time. In general, opting out/unsubscribing from emails must be easily doable for the recipient, i.e. without entering access data (e.g. login or password).
- Neither the sender nor the commercial nature of the email may be disguised or concealed in the header and/or subject line of the email. An email is considered disguised or concealed if the header and subject line are intentionally designed in such a way that the recipient receives no or merely misleading information as to the sender's actual identity or the commercial nature of the message before reading the content.

Technical Configuration

- Sender addresses must be registered and be included in the service administration. The sender address must be able to receive emails (valid DNS MX record). The sender domain must also have a valid DNS A-Record. Role-based sender addresses (e.g. abuse@ or postmaster@) are not permitted.
- The Customer must immediately delete email addresses from the respective mailing lists if non-existence of the address is discovered upon transmission, and at the latest if three hard bounces have occurred. The total hard bounce rate per ISP shall generally not exceed 1.0%. Role-based recipient addresses (e.g. postmaster@, abuse@) will be rejected/discarded.
- The Customer must delete email addresses from the respective mailing lists if the recipient categorizes an email as spam and reports this (complaint) or revokes consent to receiving emails.

- For the 'MAIL FROM' address specified in the SMTP communication between email servers, an SPF-From Record must be entered, thereby allowing an SPF test to be carried out on the recipient side. The SPF Record must end in "-all" or "~all". In case the necessary entries are not made on the Customer's side within ten (10) business days, the re-verification efforts and expenses will be charged in accordance with Retarus' agreed hourly rates.
- The use of the DKIM (DomainKeys Identified Mail) method is mandatory. For each sender domain registered with Retarus on behalf of the Customer, the Customer must store a corresponding DKIM key in their DNS. If Customer fails to make the necessary entries within ten (10) business days, the reverification will be billed in accordance with Retarus' agreed hourly rates.
- A 'List-unsubscribe'-header or a 'List-help'-header (see RFC 2369) must be included in every email. The 'List unsubscribe' header is required for list-based mailings, and has to be inserted with a 'POST HTTPS'-link including a 'One-click unsubscribe' feature (RFC 8058). The link provided must trigger a direct one-click unsubscription at least at list level. The sender may send unsubscribe confirmation emails. In non-list-based mailings, the 'List-help' header shall be set as an alternative to the 'List-unsubscribe' header. The 'List help' header shall include at least one 'mail-to' address or a HTTPS link. HTTP links are not permitted. Both the use of the "mailto" address and the HTTPS link must enable the recipient to receive information about the reason why the email was sent to them and why unsubscribing at the list level is not possible.

- Using the „list-unsubscribe-Post"-Header requires a valid URL address which can receive and process such POST requests.

  Example:

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

- Exceptions to these obligations may apply if it is not required or possible to unsubscribe as described above due to the configuration of the Service and the associated transmission of automated emails.
- The Customer must set up an abuse email address for the reporting of the abuse of email addresses for the addressees of the emails and monitor it. The abuse email address can be configured for example as abuse@domain.
- The delivery of emails to the Retarus Transactional Email service must take place via Transport Layer Security (TLS – opportunistic/enforced) from the customer, according to the current state of the technic. Retarus uses for sending emails to the addressee Transport Layer Security (TLS) while using CSA IP-addresses.
- Retarus is Certified Senders Alliance ("CSA") certified. The cooperation duties described herein reflect the current CSA requirements. The CSA reserves the right to adapt their requirements at any time, in which case Retarus will notify Customer accordingly. Customer agrees to comply with any such changes.