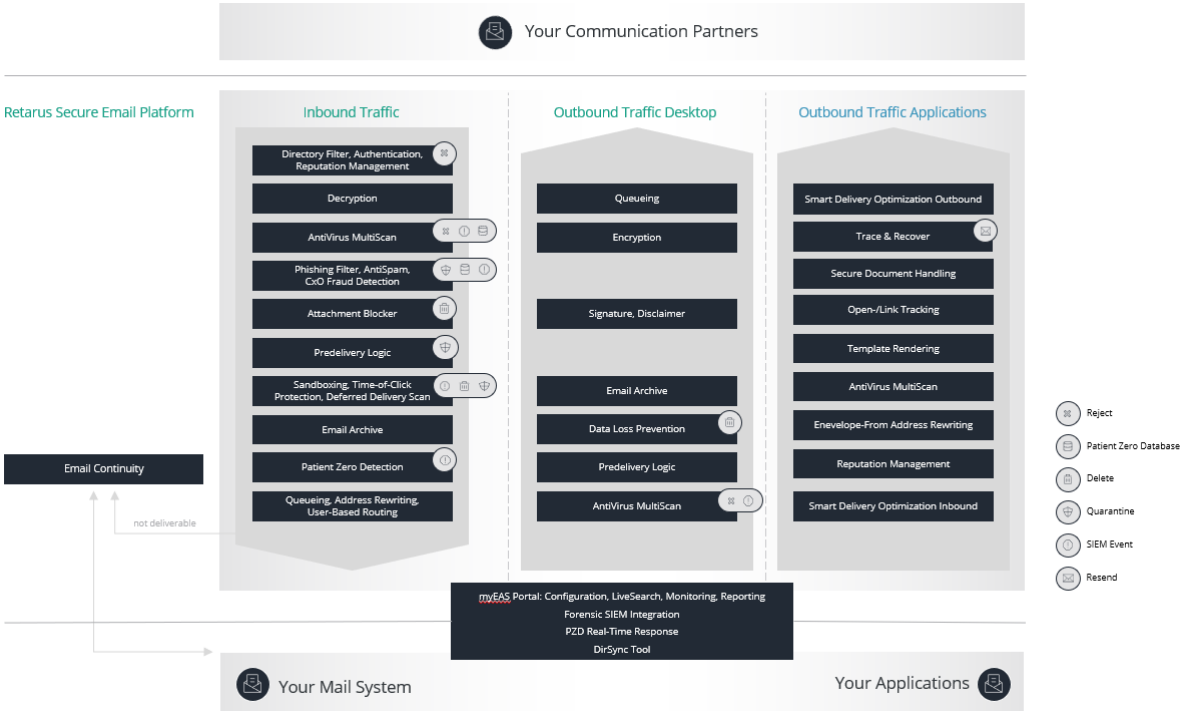
Descrizione del servizio e obblighi di cooperazione
Retarus Secure Email Platform

La piattaforma **Retarus Secure Email Platform** combina meccanismi di protezione completa, Advanced Threat Protection e il meccanismo brevettato di protezione post-trasmissione "Patient Zero Detection®" con funzionalità avanzate come Dynamic Email Routing, Email Encryption ed Email Continuity. In aggiunta a ciò, le applicazioni aziendali esistenti possono essere collegate alla piattaforma tramite i moduli Retarus Transactional Email.

L'offerta di servizi è strutturata nelle seguenti categorie di prodotti principali: **Email Cloud Gateway, Email Security, Email Compliance e Email Infrastructure**.

Sommario

Architettura di Sistema Retarus Secure Email Platform



Email Cloud Gateway

Il **Retarus Email Cloud Gateway** offre funzionalità di base per la gestione e la sicurezza del traffico di messaggi SMTP. Può essere utilizzato come servizio stand-alone, ma può anche essere ampliato utilizzando moduli aggiuntivi della Retarus Secure Email Platform.

L'Email Cloud Gateway comprende le seguenti funzionalità:

Directory Filter / Reputation Management

La funzione Directory Filter respinge conformemente a RFC (metodo Reject) le e-mail indirizzate ai destinatari non configurati nel portale Retarus Enterprise Administration Services (portale EAS). La configurazione e l'aggiornamento vengono eseguiti manualmente dal cliente tramite il portale EAS stesso o automaticamente tramite la sincronizzazione della directory, in un formato predefinito da Retarus, con rubriche e directory del cliente.

La reputazione del mittente del messaggio di posta elettronica in entrata viene controllata tramite la gestione della reputazione in entrata, che integra il Directory Filter.

L'autorizzazione del mittente viene convalidata tramite i meccanismi SPF (Sender Policy Framework) e DKIM (DomainKeys Identified Mail).

In caso di mancata convalida della mail analizzata, questa viene gestita in base alla configurazione del cliente nel portale EAS o, se attivata dal cliente, ulteriormente elaborata in base alle specifiche della politica DMARC (Domain-based Message Authentication, Reporting & Conformance) del proprietario del dominio (mittente) (azioni: Nessuna, Quarantena, Rifiuto).

Nota: L'utilizzo del DMARC richiede l'instradamento verso un record MX dedicato di Retarus.

AntiVirus Multiscan 2-stage

Retarus scansiona i messaggi in entrata e (quando prestabilito) in uscita per controllare la presenza di virus. Per effettuare queste scansioni, Retarus utilizza due sistemi di controllo selezionati tra vari fornitori. Non appena vengono resi disponibili aggiornamenti o nuove versioni di questi sistemi, Retarus li adotta immediatamente per controllare la presenza di virus. Nel caso Retarus dovesse identificare un virus, procede alla distruzione di tutti i tipi di email infette. I destinatari delle email infette e/o i loro amministratori registrati per tali occasioni sono informati come da procedura del nostro sistema di gestione della quarantena.

DHA Protection

Protezione DHA (*Directory Harvest Attack*) per il dominio o i domini e-mail selezionati dal proprietario del dominio. I messaggi a destinatari non validi all'interno del dominio interessato saranno rifiutati. La ricezione di ulteriori messaggi a destinatari non validi sarà limitata dal blocco del mittente identificato di questi messaggi.

Backscatter Protection

Protezione dall'uso improprio dei "bounce messages" generati automaticamente per l'invio (Backscatter).

Il Backscatter è l'uso non autorizzato dell'indirizzo email valido di un'altra persona per campagne di spam. Può accadere che il server di posta elettronica riceva un gran numero di notifiche di stato di consegna (ad esempio se l'indirizzo ricevente non esiste) all'indirizzo di posta elettronica valido della persona che è stata usata come mittente a sua insaputa. Le e-mail non vengono consegnate al mittente effettivo.

Grazie a Backscatter Protection, un numero maggiore di questi messaggi generati automaticamente sarà identificato e filtrato, e la loro consegna sarà impedita utilizzando l'isolamento del destinatario interessato nella quarantena personale. Nella quarantena personale, questi messaggi saranno contrassegnati come NDR Spam.

Email Back-Up / Queuing

In caso di mancato recapito dei messaggi destinati al cliente, Retarus conserverà i rispettivi messaggi in entrata per un massimo di 96 ore. Qualora non si riesca a risolvere il problema, il mittente del messaggio riceverà una notifica via email di mancato recapito. Retarus continuerà a tentare l'invio a intervalli brevi nelle 96 ore successive. Se il problema di consegna si risolve durante questo arco di tempo, i messaggi in ingresso sono inviati a Retarus in blocchi.

Large Email Handling

Le e-mail di grosse dimensioni, che superano i limiti definiti dal cliente, non vengono inviate immediatamente alle caselle di posta ma rese disponibili per il download in Retarus. Il destinatario riceve una notifica di tale ricezione, se l'opzione è configurata. Il download avviene tramite un link HTTP con autenticazione semplificata dell'utente (OneClick-Token-Login).

User based Routing

Grazie all'opzione User-based Routing (instradamento basato sull'utente), Retarus consegna a specifici server di destinazione le e-mail indirizzate a determinati destinatari presso il cliente all'interno di un dominio.

Email Signature / Disclaimer

Il cliente ha la possibilità di salvare file di firma o disclaimer all'interno del portale Enterprise Administration Services (portale EAS). Retarus allega i file di firma o il disclaimer generati tramite il portale EAS ai messaggi e-mail in uscita del cliente. I segnaposto utilizzati vengono popolati con dati provenienti dalla directory di sincronizzazione.

Email Live Search

Con Email Live Search, tutti i messaggi in entrata e in uscita possono essere tracciati in tempo reale. Per ogni e-mail è possibile ripercorrere l'eventuale infezione di un determinato virus e l'applicazione di ulteriori filtri e regole.

Access Management

Nel portale Retarus Enterprise Administration Services (portale EAS) è possibile assegnare i diritti di accesso ai singoli amministratori in base ai requisiti del cliente, ad es. con diversi diritti di accesso per determinati paesi, filiali, domini o reparti.

Email Security

Retarus Email Security consente di proteggere le infrastrutture di e-mail da malware quali virus, spam, e-mail di phishing, ransomware e altre minacce digitali. I metodi di filtro multilivello vengono costantemente aggiornati ed ottimizzati. I dati vengono elaborati nei centri di calcolo di Retarus ai sensi delle norme vigenti sulla tutela dei dati.

AntiVirus MultiScan (2 scanner)

Retarus scansiona i messaggi in entrata e (quando prestabilito) in uscita per controllare la presenza di virus. Per effettuare queste scansioni, Retarus utilizza due sistemi di controllo selezionati tra vari fornitori. Non appena vengono resi disponibili aggiornamenti o nuove versioni di questi sistemi, Retarus li adotta immediatamente per controllare la presenza di virus. Nel caso Retarus dovesse identificare un virus, procede alla distruzione di tutti i tipi di email infette. I destinatari delle email infette e/o i loro amministratori registrati per tali occasioni sono informati come da procedura del nostro sistema di gestione della quarantena.

AntiVirus MultiScan (4 scanner)

Analogamente all'AntiVirus MultiScan a due scanner, la verifica viene eseguita con quattro scanner di diversi fornitori.

External Sender Visibility Enhancement

La funzionalità External Sender Visibility Enhancement identifica i messaggi in arrivo che nel campo del mittente utilizzano un dominio mittente assegnato al cliente. Per la convalida del mittente viene utilizzato il campo di intestazione MIME-FROM. All'interno dell'infrastruttura Retarus, i messaggi in arrivo vengono contrassegnati con icone Unicode (simboli) predefinite prima di essere trasferiti all'infrastruttura del cliente. Il contrassegno viene applicato nel campo del mittente "friendly name".

Antispam Management e Phishing Filter (inbound)

Come il Retarus AntiSpam Management and Phishing Filter (Inbound), l'omologo servizio Outbound sfrutta la rinomata tecnologia di filtraggio dello spam utilizzata da Retarus. A ogni e-mail in uscita viene assegnato un punteggio di probabilità che si tratti di SPAM e quelle che superano una data soglia configurabile (60% è l'impostazione predefinita) sono soggette a diverse possibilità di smaltimento in base alle preferenze di configurazione del cliente. Le opzioni disponibili includono il rifiuto, la disabilitazione temporanea (tempfail) e lo scarto automatico, consentendo di adattare la risposta alle specifiche politiche di sicurezza del cliente. La flessibilità della configurazione si estende a tutti i livelli gerarchici, dando la possibilità di regolare con precisione le impostazioni relative non solo al cliente, ma anche al dominio, al profilo e all'utente. Per attivare la funzione, si prega di contattare il Support di Retarus.

AntiSpam Management e Phishing Filter (outbound)

Come il Retarus AntiSpam Management and Phishing Filter (Inbound), l'omologo servizio Outbound sfrutta la rinomata tecnologia di filtraggio dello spam utilizzata da Retarus. A ogni e-mail in uscita viene assegnato un punteggio di probabilità che si tratti di SPAM e quelle che superano una data soglia configurabile (60% è l'impostazione predefinita) sono soggette a diverse possibilità di smaltimento in base alle preferenze di configurazione del cliente. Le opzioni disponibili includono il rifiuto, la disabilitazione temporanea (tempfail) e lo scarto automatico, consentendo di adattare la risposta alle specifiche politiche di sicurezza del cliente. La flessibilità della configurazione si estende a tutti i livelli gerarchici, dando la possibilità di regolare con precisione le impostazioni relative non solo al cliente, ma anche al dominio, al profilo e all'utente. Per attivare la funzione, si prega di contattare il Support di Retarus.

Attachment Blocker

L’invio di determinati allegati e-mail (attachment) può essere impedito in base alle configurazioni impostate del cliente. Gli attachment da bloccare sono determinabili in base all’estensione dei file (es. exe, mp3, zip) e in base al tipo MIME corrispondente. Il file allegato di un’e-mail in arrivo viene eliminato consegnando al destinatario esclusivamente il corpo della mail oppure una copia dell’e-mail originale con allegato viene inviata a una casella di posta predefinita (es. amministratore). I destinatari possono essere informati degli attachment eliminati con notifiche configurabili.

Outbound Recipient Restriction

Di norma le e-mail in uscita elaborate da Retarus possono avere fino a 600 indirizzi di destinatari. Se un'e-mail supera questa soglia, Retarus la respinge per i destinatari in eccesso; la relativa notifica dipende dalla configurazione del server di posta elettronica del cliente. La nostra funzione Outbound Recipient Restriction consente di impostare un numero massimo a scelta di destinatari (0-600) per le e-mail in uscita. Il superamento del limite configurato può attivare il rifiuto, la disabilitazione temporanea o lo scarto automatico dell'e-mail a seconda delle preferenze del cliente. Questa funzionalità mira a limitare i destinatari prevenendo così l'esposizione dell'identità del cliente e facilitando una gestione efficiente. Questa funzione può essere configurata a tutti i livelli gerarchici (cliente, dominio, profilo, utente). Per attivarla è inizialmente necessaria l'assistenza del Support di Retarus.

Outbound Size Restriction

Di norma le e-mail in uscita elaborate da Retarus possono avere una dimensione massima di 250 MB (256000 kB). La funzione "Outbound Size Restriction" permette al cliente di limitare ulteriormente le dimensioni delle e-mail in uscita (Outbound) ove necessario. Il superamento del limite configurato può attivare il rifiuto, la disabilitazione temporanea o lo scarto automatico dell'e-mail a seconda delle preferenze del cliente. Questa funzione può essere configurata a tutti i livelli gerarchici (cliente, dominio, profilo, utente). Per attivarla è inizialmente necessaria l'assistenza del Support di Retarus.

Deferred Delivery Scan

Nell'ambito della funzione Deferred Delivery Scan (DDS) determinati file allegati vengono sottoposti a un'ulteriore analisi tramite procedure aggiuntive di riscansione. Tali nuovi scansioni con file di firma più aggiornati impediscono con maggiore probabilità l'invio di contenuti dannosi non ancora riconosciuti al momento della prima scansione. Se viene stabilito un attacco virus, Retarus elimina i messaggi corrispondenti e fornisce informazioni in base alla configurazione impostata nella gestione della quarantena. Poiché la funzione DDS implica un ritardo nell'invio delle e-mail in arrivo, non risultano quindi validi gli eventuali livelli di assistenza concordati relativamente ai tempi di invio.

Time-of-Click Protection

I link contenuti nelle e-mail vengono automaticamente sovrascritti (URL-Rewriting). Se i destinatari fanno clic sui link corrispondenti, viene verificato che non siano indirizzi sospettosi di phishing. Se la pagina di destinazione non viene riconosciuta come phishing, viene eseguito un inoltro diretto. In caso contrario, viene visualizzato un avviso di sicurezza. In ogni caso, alla cessazione del servizio, i link corrispondenti non possono più essere consultati immediatamente.

CxO Fraud Detection

CxO Fraud Detection utilizza algoritmi che identificano "From Spoofing" e "Domain Spoofing" per riconoscere indirizzi di mittenti falsificati (es. di superiori di alto livello). I messaggi classificati come CxO Fraud vengono gestiti in base alla configurazione nella gestione della quarantena.

Sandboxing

La funzione Sandboxing sottopone determinati file allegati a un'ulteriore analisi. Gli attachment, che possono presentare contenuti dannosi, vengono eseguiti in una macchina virtuale che ne verifica il comportamento inconsueto. Per questo tipo di verifica, Retarus utilizza soluzioni Sandbox di un fornitore terzo specializzato. Se viene rilevata un'infestazione con contenuti dannosi, i messaggi corrispondenti vengono gestiti in base alla configurazione nella gestione della quarantena. Poiché la funzione Sandboxing può implicare un ritardo nell'invio delle e-mail in arrivo in funzione tra l'altro delle dimensioni del file, del tipo di file e del numero di file allegati, non risultano quindi validi gli eventuali livelli di assistenza concordati relativamente ai tempi di invio.

Patient Zero Detection®

All'arrivo delle e-mail indirizzate ai destinatari del cliente, Patient Zero Detection® crea un'impronta digitale ("hash") di tutti i file allegati e link. Se gli scanner antivirus impostati da Retarus riconoscono, in un secondo momento, contenuti dannosi in un allegato o link dello stesso genere, è possibile identificare anche i destinatari di messaggi potenzialmente dannosi già inviati. Gli amministratori del cliente e, in base all'incarico, anche direttamente i destinatari di tali messaggi vengono immediatamente informati di tale circostanza. Il cliente viene così messo nelle condizioni di intervenire tempestivamente per eliminare il malware dalla propria infrastruttura o per prevenirne la diffusione.

Patient Zero Detection® Real-Time Response

Con Patient Zero Detection® Real-Time Response, Retarus fornisce un software che i clienti possono gestire all'interno della loro infrastruttura. Il software gestisce automaticamente i messaggi che sono stati identificati come nocivi dal Patient Zero Detection® nel momento del recapito alla casella di posta del destinatario. Successivamente, tali messaggi possono essere rimossi automaticamente dalla casella di posta del destinatario. Presupposto per il funzionamento di Patient Zero Detection® Real Time Response è l'utilizzo di "Retarus Forensic SIEM Integration" e la connessione del cliente a Microsoft Exchange. Patient Zero Detection® Real-Time Response è soggetta a speciali condizioni d'uso, che il cliente deve rispettare durante l'installazione o l'utilizzo del software. Tali condizioni di utilizzo sono consultabili nel portale EAS.

Quarantine Management

All'interno della gestione della quarantena, il cliente o (se lo desidera) i suoi singoli utenti, possono definire l'invio in determinati momenti di un report di Email Security (Digest). In base alle opzioni configurate, Digest comprende una panoramica combinata di e-mail che Retarus provvede a mettere in quarantena o a eliminare in base a graymail (es. newsletter), virus, spam, phishing, sandboxing, CxO Fraud ecc. entro il periodo impostato. I messaggi messi in quarantena sono consultabili dal cliente facendo clic sulla voce corrispondente in Digest entro il periodo impostato (massimo 30 giorni). Se il cliente ha provveduto a tale preimpostazione, i singoli destinatari possono accedere alla quarantena online e definire impostazioni personali. Gli amministratori del cliente possono configurare le impostazioni di quarantena dell'intero sistema nel portale Enterprise Administration Services (portale EAS).

Forensic SIEM Integration

Nell'ambito di Forensic SIEM Integration, Retarus mette a disposizione un'interfaccia che consente al cliente di richiamare informazioni su eventi e risultati (Event o Log) derivanti dalla verifica di messaggi in entrata e in uscita all'interno di Retarus Email Security. Queste possono essere integrate in uno strumento SIEM esistente come fonte di dati aggiuntiva. Gli eventi forniti al cliente dipendono dalle opzioni riservate e sono disponibili per:

- AntiVirus MultiScan (Inbound e Outbound)
- Sandboxing
- CxO Fraud Detection
- Patient Zero Detection®
- E-mail in uscita in generale
- E-mail in arrivo, in generale

Email Compliance

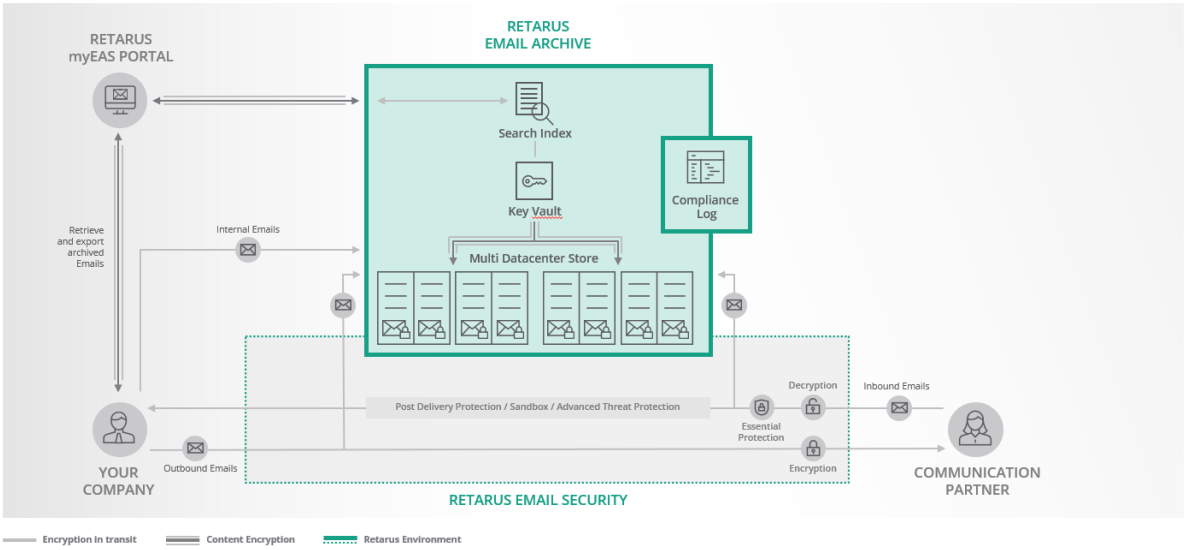
Retarus Email Archive

Retarus Email Archive conserva le comunicazioni via email in entrata e uscita in modo automatico, affidabile e nel lungo termine. Se necessario, Retarus Email Archive può conservare anche le comunicazioni interne via email.

I messaggi consegnati a Retarus Email Archive non sono modificabili e sono protetti da accessi e recuperi non autorizzati. Questi messaggi sono conservati fino al termine dell'accordo commerciale, per un massimo di dieci anni, e saranno eliminati al termine della durata prestabilita dalle parti nel rispetto delle leggi, a meno che non siano stati stipulati accordi diversi. Durante il periodo di archiviazione, i clienti possono trovare e inviare nuovamente le email con facilità, grazie a diverse opzioni di filtro. Se il cliente desidera esportare l'intero archivio prima del termine del periodo di archiviazione prestabilito e la sua conseguente eliminazione, è necessario che ne faccia richiesta prima del termine temporale dell'accordo.

L'accesso dell'amministratore all'archivio delle email si basa sul principio di doppio controllo. Email e allegati archiviati sono facili da trovare, utilizzando potenti funzionalità di ricerca, che, se necessario, possono essere rifinite a livello granulare, ad esempio per rispettare gli obblighi di protezione dei dati.

Sarà automaticamente creato un protocollo completo di accesso.



Funzionalità:

- Conservazione affidabile di tutte le email in entrata e uscita
- Conservazione sicura e non modificabile, basata su una crittografia ibrida
- Informazioni di tracciamento con EAS Live Search
- Protocollo di accesso creato automaticamente
- Assistenza per rispettare i requisiti normativi
- Messaggi recuperabili con allegati inclusi
- Accesso basato su un principio di doppio controllo tramite il portale amministrativo Retarus, basato sul web
- Potenti funzionalità di ricerca con un'opzione di configurazione per il rispetto della protezione dei dati: Ricerca delle email in base a mittente, destinatario o formato del file in allegato; archiviazione configurabile dei rispettivi (meta)dati per ricerche in base a oggetto, al testo nel corpo o al nome dell'allegato

Opzioni su richiesta

- Archiviazione delle comunicazioni interne via email tramite Journaling (Microsoft Exchange o M365 Exchange Online)
- Accesso comodo e sicuro per gli amministratori del cliente tramite Single Sign-on
- Importazione delle email da altri sistemi di archiviazione (idealmente in formato eml)
- Esportazione delle email archiviate in un archivio dati esterno
- Utilizzo delle chiavi (pubbliche) del cliente stesso (le chiavi private rimangono al cliente)

Retarus Email Encryption

Retarus Email Encryption aiuta i clienti a garantire l'integrità, l'autenticità e la riservatezza dei messaggi e-mail. A tal fine, le e-mail (compresi gli eventuali allegati) vengono crittografate automaticamente, come richiesto dal sistema Retarus secondo regole predefinite o controllate dall'utente, e/o firmate secondo necessità, prima di essere inviate al destinatario. Viene eseguito un controllo antivirus commissionato per i messaggi in uscita prima della crittografia e per i messaggi in entrata dopo la decritto grafia.

Funzionalità aggiuntive:

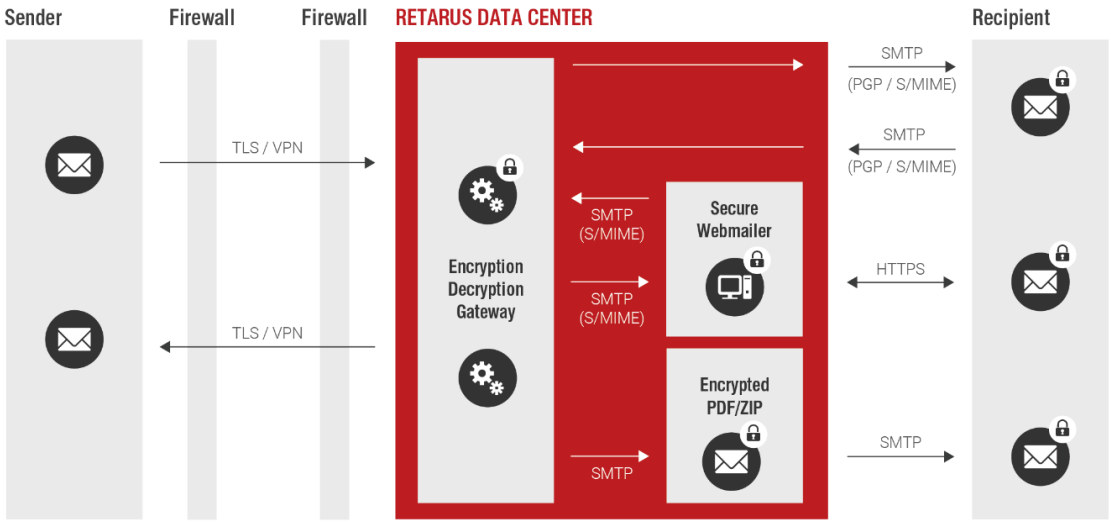
- Adozione delle Public Key Infrastructure (PKI) esistenti
- Ulteriore utilizzo dei certificati S/MIME esistenti e validi
- Supporto degli standard Open PGP, PGP e S/MIME
- Integrazione delle politiche di crittografia del cliente
- Fornitura di add-in per Microsoft Outlook per controllare le azioni degli utenti riguardanti crittografia e/o firma dei messaggi
- Fornitura di metodi alternativi di comunicazione criptata tramite Retarus Secure WebMailer, oppure con l'invio di file PDF o ZIP criptati
- Integrazione facoltativa di un Trust Center ufficiale (attualmente SwissSign) per creare certificati S/MIME in base allo standard X.509
- Sincronizzazione automatizzata degli utenti per creare e rinnovare certificati (su richiesta)

User Synchronization for Encryption (USE)

User Synchronization for Encryption (USE) è una soluzione che semplifica la gestione di utenti e gruppi di encryption, così come delle relative chiavi S/MIME o PGP. Con l'obiettivo di migliorare l'esperienza dell'utente e ridurre l'intervento manuale, USE automatizza il processo di rinnovo, verifica e revoca di certificati e chiavi, monitorando le date di scadenza e avviando gli interventi necessari.

- È in grado di importare in modo sicuro gli utenti di encryption e di assegnarli a gruppi predefiniti.
- Gestisce le politiche sulla base dei requisiti dei clienti e dei gruppi di utenti.
- Automatizza la creazione/revoca e la sincronizzazione di S/MIME (SwissSign).
- Distingue tra certificati personali e di team per evitare disfunzioni.
- Consente una ricertificazione interamente automatizzata o semiautomatizzata.
- Crea/elimina le chiavi PGP e sincronizza le chiavi private corrispondenti per ciascun utente.
- Consente l'importazione di chiavi/certificati creati/acquistati separatamente dai clienti.
- Annota le regole per la gestione dei criteri di encryption del cliente in modo che siano accessibili anche al lettore umano.
- È in grado di generare report di sincronizzazione e report transazionali S/MIME a scopi di conformità e verifica.
- I report possono essere ricevuti via e-mail o memorizzati sulla condivisione SFTP per essere ritirati.

Architettura di Sistema Retarus Email Encryption



Digital Signature / Certificates

Con Retarus Email Encryption, i messaggi e-mail in uscita possono essere firmati con chiavi PGP o certificati S/MIME in base a necessità o automaticamente come da normativa. Nel caso di messaggi in arrivo, l'utente può facilmente riconoscere il risultato della verifica della firma grazie alla trasparenza delle informazioni. Oltre ai certificati standard X.509 S/MIME (certificati e-mail di classe 2), possono essere utilizzati anche certificati S/MIME opzionali di un Trust Center (attualmente SwissSign). Tali certificati vengono forniti tramite il Managed PKI (MPKI). Il prerequisito è che, oltre alle condizioni di Retarus, vengano accettate anche altre condizioni del Trust Center.

Secure WebMailer

Secure WebMailer è un portale web sicuro, attraverso il quale i clienti possono scambiare e-mail criptate con interlocutori che non utilizzano S/MIME o PGP. Con un link è possibile accedere a una casella di posta individuale/personale creata automaticamente a tale scopo in Retarus Secure WebMailer. Tutti gli accessi sono criptati in HTTPS. Sia le modalità di trasmissione (via e-mail o SMS*) dei dati personali di accesso al rispettivo mittente e destinatario dei messaggi e-mail, sia l'eventuale gestione di Secure WebMailer personalizzata specificatamente per l'azienda, vengono definite insieme al cliente durante il workshop iniziale sulla crittografia dei messaggi e-mail.

Encrypted PDF /ZIP

Retarus offre la possibilità di trasmettere informazioni riservate sotto forma di un documento PDF o di un file ZIP, entrambi protetti da password. Il testo dell'e-mail, compresi tutti gli allegati, è integrato in un file PDF o ZIP, che viene crittografato e inoltrato al destinatario. L'invio della password per l'apertura del documento PDF o del file ZIP e l'adattamento opzionale del modello utilizzato sono definiti insieme al cliente durante il workshop iniziale sulla crittografia dei messaggi e-mail.

Initial Email Encryption workshop

Il workshop iniziale sulla crittografia dei messaggi e-mail è un prerequisito necessario per la configurazione di Retarus Email Encryption. Nel workshop, il cliente collabora con Retarus per definire i requisiti specifici del cliente per la configurazione. I contenuti possono includere:

- introduzione alla crittografia,
- presentazione delle norme stabilite,
- inventario delle infrastrutture esistenti,
- analisi dei requisiti specifici del cliente e delle linee guida di sicurezza,
- definizione di flussi di lavoro e processi, ad esempio per quanto riguarda la crittografia/firma o la raccolta di chiavi pubbliche,
- definizione del layout e del contenuto delle notifiche e-mail,
- definizione dell'utilizzo di Secure WebMailer (ad es. trasmissione di dati di accesso),
- definizione dell'utilizzo di un documento PDF criptato (ad es. la trasmissione della password).

Sulla base dei risultati, il client di crittografia specifico del cliente viene configurato nel sistema Retarus in linea con gli standard S/MIME e PGP o con metodi di crittografia alternativi (Secure WebMailer/PDF criptato).

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

L'elaborazione di messaggi generati da macchine e/o da automatismi fissi, applicazioni di portali o soluzioni correlate al processo (ad es. un modulo di firma) avviene tramite una cosiddetta licenza eBusiness. A ogni indirizzo di mittente di tale applicazione viene assegnata una licenza d'uso eBusiness separata. Con l'utilizzo opzionale dei certificati S/MIME, Retarus gestisce per conto del cliente i certificati di classe 2 della categoria "Silver".

Data Loss Prevention

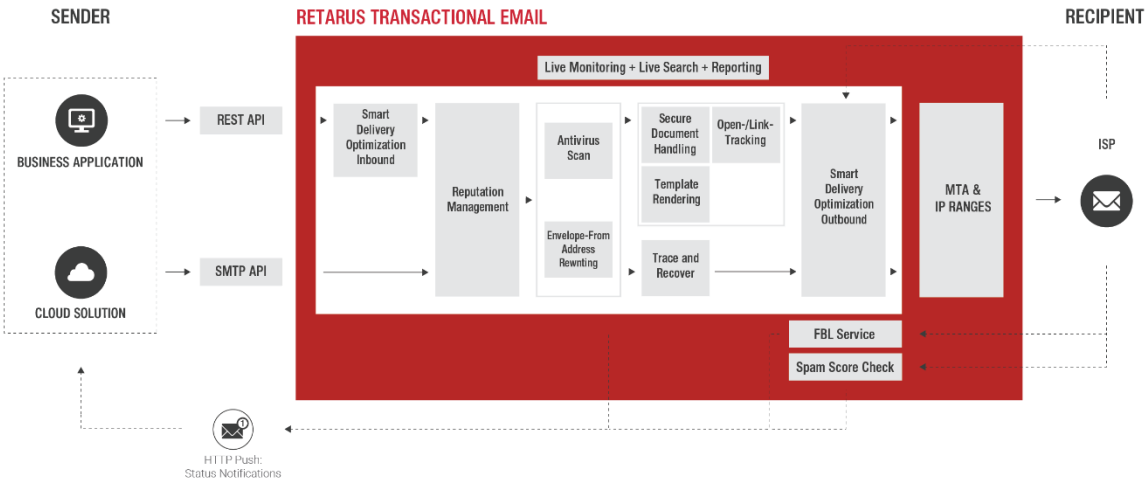
Data Loss Prevention verifica le e-mail indirizzate a destinatari esterni da utenti del cliente sui modelli definiti nell'ambito della configurazione, ad es. numeri di carta di credito o numero di conto corrente (IBAN). Se un'e-mail contiene tali modelli, viene impedita la trasmissione a destinatari esterni. Inoltre, è possibile informare determinati dipendenti, ad es. un amministratore o un Compliance Officer, relativamente al tentativo di invio. L'e-mail in questione sarà allegata alla notifica. In via facoltativa, è possibile informare anche il mittente stesso. La verifica di tali modelli comprende il corpo dell'e-mail. Inoltre, è possibile impedire l'invio degli allegati in base all'estensione dei file (es. exe, mp3, zip) e in base al tipo MIME corrispondente. Inoltre, è possibile impostare l'opzione di invio delle e-mail a destinatari esterni solo se viene introdotta un'istanza di controllo, ad es. una casella di posta funzionale, nel ripartitore.

Email Infrastructure

Retarus Transactional Email

Con **Retarus Transactional Email** è possibile inviare grossi volumi di email direttamente dalle applicazioni aziendali, senza pesare sull'infrastruttura del cliente. A questo scopo, l'infrastruttura del cliente sarà collegata a Retarus Enterprise Cloud tramite interfacce standard. I dati sono elaborati nei centri dati di Retarus.

Architettura di sistema 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

*Queste funzionalità richiedono l'utilizzo di indirizzi IPv4.

Basic Configuration

La configurazione del servizio base include l'accesso ai dati o un'autenticazione IP registrata per un end point EPI o un server SMTP in un data center Retarus. Le comunicazioni avranno luogo utilizzando una connessione sicura tramite HTTPS e/o SMTP Auth Basic tramite eTLS. L'installazione include dominio/indirizzo del mittente, parametri predefiniti del lavoro, routing IP, record SPF e firma DKIM. L'account verrà attivato quanto verrà configurato completamente e con successo e quando verrà fornita la descrizione di interfaccia.

*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

A uno o più domini del mittente sarà assegnato un indirizzo IP dedicato. Questo permette che il traffico email da diverse applicazioni venga separato, così come società madri e filiali, e che le regioni vengano divise. È consigliato utilizzare un indirizzo Dedicated IP qualora venga inviato un minimo di 1.000.000 di email al mese. Dato che il Transactional Email Service è generalmente connesso a un gruppo di data center (Active/Active), l'utilizzo di un Dedicated IP richiede almeno due indirizzi IP dedicati. Quando gli indirizzi IP appositi saranno configurati, Retarus fornirà gli indirizzi IPv4 al cliente, da utilizzare per tutta la durata del contratto. Questi verranno integrati nel Blacklist Monitoring System di Retarus. Retarus potrà in ogni momento scambiare gli indirizzi IP.

Enforced TLS

Durante la configurazione base del servizio, verrà determinato, a livello di dominio di spedizione, se sarà necessario utilizzare un encryption protocollo ibrido per ciascuna email inviata. In questo modo, ci proponiamo di configurare una connessione criptata, non appena il cliente invierà email tramite il dominio fornito (enforced TLS). Se il destinatario non accetterà la connessione criptata, la procedura di invio sarà annullata.

Envelope From Address Rewriting (Outbound)

In alternativa, Retarus offre una Envelope From Address Rewriting per le email in uscita, al fine di reindirizzare le potenziali risposte in una cartella apposita. La riscrittura degli indirizzi è particolarmente utile se, ad esempio, le politiche aziendali non permettono di inviare email in Internet tramite il dominio stesso dell'azienda.

Account / Access Token

Un account è definito come un'unità di autenticazione (definizione di nome utente/password API, ecc.) ed è collegato a uno specifico centro dati, punto di accesso API. Per ogni account è possibile gestire più domini. È anche possibile gestire lo stesso dominio con più account.

Smart Delivery Optimization

Retarus utilizza la gestione intelligente di invio e ricezione email, in base al dominio di spedizione. Smart Delivery Optimization adatta automaticamente il comportamento di spedizione del cliente alle risposte dei singoli ISP e/o ESP, al fine di mantenere alta la capacità di messaggio per ISP e/o ESP. In casi eccezionali, la gestione ottimizzata può portare a una riduzione della capacità di elaborazione accordata.

Status Information via API Callback (Webhook)

Informazioni sullo stato via API Callback (Webhook). Il cliente verrà informato della creazione di nuovi eventi, come stati di consegna, ragioni per la mancata consegna, blocco dell'invio ai destinatari nella Suppression List, oltre a informazioni sul tracciamento delle aperture e dei link. Questi tipi di informazioni di stato possono essere integrati automaticamente nei processi aziendali e nelle applicazioni via HTTP POST, ad esempio per mantenere i dati sorgente (igiene del database) o supportare la reputazione dei domini del cliente.

Retarus EAS – Live Monitoring

Retarus offre Live Monitoring nel suo portale EAS, attraverso il quale le email possono essere tracciate in tempo reale. Grazie a questa soluzione, il cliente possono valutare lo sviluppo di tendenze nelle aree di consegna, soft e hard bounce e messaggi scartati, attivando le contromisure più adatte.

Retarus EAS – Live Search

Retarus EAS Live Search fornisce una panoramica trasparente delle tue email inviate. EAS Live Search consente di trovare email in uscita utilizzando lassi di tempo, ID messaggi, mittenti e destinatari, nonché di ricevere informazioni dettagliate sullo stato degli ultimi 45 giorni.

Retarus EAS – Reporting

Retarus EAS Reporting ti fornisce una panoramica trasparente delle email inviate negli ultimi 45 giorni, scaricabile in file CSV o Excel (XLSX).

Smart Network Data Service – Report (SNDS)

Gli Smart Network Data Services (SNDS) ti forniscono i dati di cui hai bisogno per comprendere la tua reputazione su Microsoft e migliorarla. SNDS ti garantisce l'accesso a dati dettagliati degli indirizzi IP da te utilizzati in formato CSV. Questo servizio può essere utilizzato in connessione con un indirizzo Dedicated IP.

E-Mail Reporting (CSV)

Retarus offre un rapporto di spedizione in formato CSV tramite il Portale Enterprise Administration Services (portale EAS) Questi rapporti sono disponibili al cliente su base giornaliera e per un periodo di 180 giorni. Questi rapporti includono solamente transazioni con uno status finale. Le transazioni che devono ancora essere elaborate non sono elencate. Il rapporto è accessibile in diversi file oppure come cartella compressa (ad esempio in formato ZIP).

Nota: la configurazione di un rapporto CSV ci richiede di conservare temporaneamente i dati ai fini della fornitura di servizi. I dati conversati includono informazioni sull'elaborazione dei messaggi, così come dati personali quali gli indirizzi email dei mittenti e dei destinatari, ma non i contenuti.

Retarus Spam Score Check

La possibilità che i messaggi vengano categorizzati come spam dipende da diversi fattori. Formattazione HTML insolita o strutture delle tabelle, numero eccessivo di link o diciture di dubbia natura, nell'oggetto o nel corpo del testo, possono generare avvisi di spam. A questo proposito, Retarus offre un servizio di Spam Score Check a pagamento. Il servizio ti consente di controllare - prima di inviare la tua email - quanto sia probabile che questa venga categorizzata come spam. Lo Spam Score viene restituito tramite una procedura automatica che ritrasmette determinate informazioni da parte di Retarus tramite email, all'indirizzo di risposta da te fornito o tramite l'API Callback sul tuo servizio web disponibile. A seguito dell'esecuzione della trasmissione, tutte le informazioni relative alla stessa verranno eliminate e non saranno conservate.

Open and Link Tracking (optional CNAME)

La funzione Open Tracking ti consente di determinare il tasso di apertura delle email, mentre il Link Tracking ti permette di determinare il tasso di apertura dei link contenuti nelle email. Per questo servizio, il corpo dell'email o il link rispettivo sarà modificato in modo tale da permettere la valutazione dei messaggi. Al fine di ridurre la probabilità che le tue email vengano classificate come spam, Retarus consiglia di prenotare il servizio CNAME. Questo permette al cliente di utilizzare uno dei suoi (sub)domini. Il cliente configura un record A del sub(dominio) nell'indirizzo di un server di Retarus. Il cliente deve informare i rispettivi destinatari delle email di Open e Link Tracking attraverso una adeguata informativa della privacy e deve ottenere in anticipo il consenso, ove necessario, in ottemperanza con le normative vigenti.

AntiVirus MultiScan

Retarus verifica l'esistenza di virus durante la procedura di invio. Il cliente può determinare in anticipo se controllare solamente gli allegati e/o il corpo dell'email. Questo controllo è svolto utilizzando due scanner antivirus di due diversi fornitori selezionati da Retarus. Non appena tali fornitori offriranno aggiornamenti o nuove versioni, Retarus le utilizzerà il prima possibile per controllare la presenza di virus. Se viene trovato un virus in un'email, Retarus la cancellerà. Informazioni relative allo stato delle email in cui è stato riscontrato un virus saranno fornite tramite l'API Callback (Webhook).

Secure Document Handling

Gli allegati per le email inviate possono essere criptati utilizzando il Secure Document Handling. A tal fine, gli allegati saranno automaticamente raggruppati in un archivio ZIP protetto da password, nell'infrastruttura Retarus, prima dell'invio. Le password saranno fornite ai destinatari in email separate. Al fine di offrire la protezione migliore al tuo destinatario, questo servizio è disponibile solo se combinato con il nostro servizio Outbound AntiVirus MultiScan.

Trace and Recover

Questa funzionalità marca le email inviate tramite una connessione SMTP come messaggi Trace & Recover. I messaggi marcati Trace & Recover sono conservati in archivi a breve termine, per 45 giorni; durante questo periodo, si possono trovare utilizzando la funzione Retarus EAS Live Search. I messaggi marcati hanno un’anteprima di 1.000 caratteri. Prima che un messaggio possa essere nuovamente inviato, se necessario, è possibile modificare solamente il destinatario iniziale.

La funzione aggiuntiva Trace & Recover necessita di AntiVirus MultiScan, ed è attivata da Retarus per un conto tecnico stabilito dal cliente. Trace & Recover non può essere utilizzato insieme a Envelope-From Address Rewriting (in uscita).

Processing Capacity

Le capacità di elaborazione sono calcolate utilizzando la configurazione base dl Transactional Email. Questo prevede una dimensione di 200 KB ed include Open e Link Tracking, per un periodo pari a un'ora.

La capacità di elaborazione è calcolata costantemente per ogni minuto di un'ora. Considerati possibili picchi di spedizione, la capacità di elaborazione reale potrebbe essere 1,25 volte la capacità concordata.

In caso di caratteristiche aggiuntive o email più grandi, la velocità potrebbe diminuire. Un aumento della capacità di elaborazione permette al cliente di raggiungere una performance oraria più elevata. Si tratta di una prestazione massima per l'elaborazione di messaggi presso Retarus. Sono possibili deviazioni. Al fine di aumentare la capacità di elaborazione, sono necessarie personali verifiche dei requisiti.

Example: Processing Capacity

Nel seguente esempio, la capacità di elaborazione concordata per contratto è di 150.000 e-mail/ora:

- (150.000 email/ora) / (12 x intervallo*/ora) = 12.500 email/intervallo*
- L'estensione massima per i picchi di invio del 25% può aumentare la capacità di elaborazione fino a un massimo di 15.625 email/intervallo*.

*Un intervallo è di 5 minuti.

IP Whitelisting

L'utilizzo della funzione Retarus Whitelisting ti permette di migliorare la sicurezza della tua "spedizione consentita". Sei tu a definire espressamente quali applicazioni nel tuo network sono autorizzate a utilizzare il servizio di Transactional Email, e quali non lo sono.

Feedback Loops

Retarus comunica con diversi fornitori di servizi Internet, utilizzando un accordo di reclamo. Le informazioni sui reclami saranno riportate a Retarus dagli ISP coinvolti sotto forma di Feedback Loops (ARF).

I Feedback Loops sono un meccanismo fornito dagli ISP per informare i mittenti non appena i loro messaggi vengono classificati come posta indesiderata. Con "Indesiderata" ci riferiamo a quando il tuo messaggio viene classificato come spam dal destinatario dell'email (per esempio, cliccare su "Sposta in spam" nella propria casella di posta).

Il feedback di reclamo viene svolto tramite una procedura automatica in cui le informazioni di reclamo trasmesse vengono lette e ritrasmesse tramite email al tuo indirizzo di risposta o tramite l'API Callback sul tuo servizio web disponibile. A seguito dell'esecuzione della trasmissione, tutte le informazioni relative al reclamo verranno eliminate e non saranno conservate.

Billing

Le tariffe delle email vengono calcolate per unità, dove quest'ultima corrisponde a 200 kilobyte. Ai fini della risoluzione, email più grandi di 200 kilobyte verranno divise in diverse unità.

Ad esempio: Un'email da 2403 kilobyte (circa 2,4 MB) equivale a 13 unità di tariffazione.

Le email vengono fatturate (codice: ID email) indipendentemente dalla riuscita della trasmissione (es. se le email vengono bloccate o respinte).

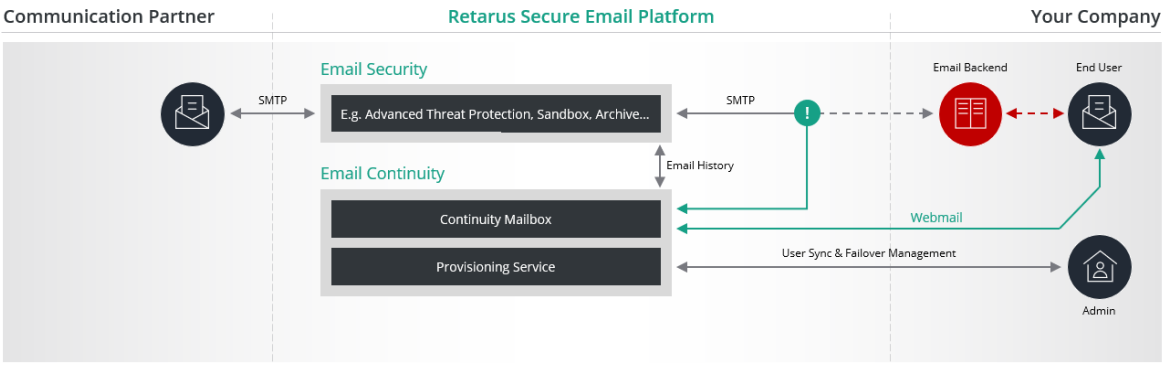
Retarus Email Continuity

Retarus Email Continuity è una piattaforma di posta elettronica alternativa per il mantenimento della comunicazione e-mail in scenari di emergenza (ad esempio, infiltrazioni di malware, guasti ai data center, inattività del cloud). Se necessario, su richiesta del cliente è possibile instradare attraverso questa piattaforma tutte le e-mail in entrata e in uscita.

Funzionalità aggiuntive:

- accesso alla casella di posta elettronica di continuità via Webmail (HTTPS),
- accesso amministrativo al servizio di provisioning, per la gestione degli utenti delle caselle di continuità,
- self-service delle password tramite una pagina di destinazione,
- trasferibilità delle e-mail dalla casella di Email Continuity (sincronizzazione inversa), su una riconsegna dei messaggi dalla casella di posta elettronica Email Continuity all'ambiente produttivo del cliente.
- Funzionalità di directory interna per visualizzare e trovare tutte le informazioni di contatto trasmesse all'interno del dominio del cliente interessato.
- Accesso amministrativo al servizio Continuity tramite REST API per la gestione degli utenti della mailbox di continuità.
- Configurazione della casella di posta elettronica tramite la Directory-Synchronization di Retarus tramite un file csv
- Notifica automatica dei nuovi utenti di Continuity aggiunti
- Self-service della password tramite una landing page (tramite token di sicurezza che i clienti gestiscono)
- Back-transmissability dei messaggi di posta elettronica dalla mailbox di continuità (Backsync) all'ambiente produttivo.
- Accesso opzionale a tutti i messaggi in entrata degli ultimi giorni (storia delle email fino a 14 giorni) secondo i domini assegnati al cliente. A tal fine è necessario un riferimento ai record MX specifici del cliente all'infrastruttura Retarus

Architettura di sistema Retarus Email Continuity



Retarus Predelivery Logic

Con la Retarus Predelivery Logic viene influenzata l'elaborazione dei messaggi all'interno dell'infrastruttura Retarus, prima della consegna all'infrastruttura del cliente. specifico per il cliente

La configurazione definita dal cliente avviene tramite la creazione di regole individuali nel portale EAS, fatte di "condizioni" e "azioni". Ad esempio, il Routing e la riscrittura possono essere effettuati in base a determinate informazioni dell'header come il mittente, l'utente o l'oggetto del messaggio.

Connection to Retarus

I sistemi del cliente vengono normalmente collegati all'infrastruttura di Retarus con il protocollo crittografico di internet Transport Layer Security (TLS) per garantire una trasmissione sicura dei dati tramite SMTP. In base alle opzioni acquistate sono possibili anche opportunistic TLS, enforced TLS o il collegamento tramite una Virtual Private Network (VPN).

Presupposto per una connessione via VPN è un collegamento simultaneo ai data center di Retarus a Monaco e a Francoforte sul Meno (RZ DE 1 e RZ DE 2).

Note

La protezione da messaggi in arrivo e in uscita con contenuto potenzialmente dannoso, compresi link integrati e allegati, si basa principalmente su procedure statistiche e di approssimazione. Nonostante l'utilizzo di tutte le caratteristiche prestazionali descritte, è possibile che si verifichi il recapito di messaggi potenzialmente dannosi, erroneamente rifiutati o erroneamente dichiarati.

Inoltre, Retarus segnala che la procedura di messa in quarantena, indipendentemente dal tipo di utilizzo dell'e-mail e dalle impostazioni personalizzate, può implicare che i messaggi, in particolare i cosiddetti "false positive", vengano recapitati in ritardo o non vengano recapitati affatto causando così eventuali svantaggi al cliente.

Le seguenti opzioni di servizio presuppongono un 4x AntiVirus MultiScan:

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

Salvo diverso esplicito accordo scritto, l'uso di Retarus Email Encryption è limitato alle comunicazioni aziendali generate di persona. L'elaborazione di messaggi generati da macchine e/o applicazioni presuppone l'intervento dell'utente eBusiness di Retarus Email Encryption.

Implementing, change management and support

L'implementazione decorre dall'assegnazione dell'ordine e dall'invio del setup sheet debitamente e correttamente compilato da parte del cliente.

Per le richieste di supporto e di assistenza, nonché per le richieste di modifica, il cliente deve segnalare a Retarus le persone formalmente autorizzate a presentare tali richieste. Il linea di massima, verrà considerato come prima persona di contatto autorizzata il referente tecnico del cliente che si occupa dell'implementazione del servizio. In qualità di amministratore del cliente, la suddetta persona potrà quindi inserire e autorizzare ulteriori contatti di supporto nel portale Enterprise Administration Services. Gli amministratori dei clienti possono modificare, estendere o cancellare queste autorizzazioni in qualsiasi momento.

Le modifiche al servizio e le soluzioni per gli incidenti (inclusi i workaround) attuate per conto del cliente devono essere accettate dal cliente almeno in forma scritta. In caso di mancata risposta da parte del cliente entro 10 giorni, il corrispondente ticket del cliente viene automaticamente chiuso e la modifica/soluzione viene considerata accettata.

Duties of Cooperation

Il cliente riconosce che l'utilizzo corretto dei servizi di Retarus e la qualità del servizio fornito dipendono molto dalla cooperazione del cliente. Il cliente, quindi, invierà il modulo di implementazione debitamente compilato, che gli è stato fornito alla stipula del contratto, entro 5 (cinque) giorni lavorativi; il cliente rispetterà in particolare gli obblighi di cooperazione stabiliti in questo documento e accetta che Retarus potrebbe adottare misure tecniche utili per assicurare una stabile fornitura dei servizi e mantenere la reputazione degli ISP delle parti. Per questo motivo, Retarus ha l'espressa autorizzazione a scartare determinati ordini di email, restringerne il volume o, in casi estremi, impedirne l'accesso. Nel caso sia necessario compiere sforzi e/o sostenere costi derivanti dal mancato rispetto degli obblighi di cooperazione, il cliente ne sarà ritenuto interamente responsabile.

Il Cliente si impegna a inviare e-mail esclusivamente a destinatari che, in base al quadro normativo e legale applicabile, abbiano dato il loro consenso esplicito (opt-in) a ricevere tali e-mail, a meno che non esistano altre autorizzazioni legalmente riconosciute. Il Cliente si impegna a rispettare i requisiti di notifica, le dichiarazioni sulla privacy, ad esempio nel contesto dell'Open o Link Tracking - o altrimenti, se applicabile - in conformità alle leggi e ai regolamenti applicabili.

Design dell'email

Ciascuna email inviata dovrà includere una sigla all'interno del corpo testuale, che rispetti le normative vigenti e sia facilmente riconoscibile.

Inoltre, si applica ciò che segue alle email inviate con contenuti promozionali:

- Il mittente dell'email promozionale deve essere ben visibile.
- In ciascuna email, il destinatario deve essere informato separatamente circa la possibilità, in qualunque momento, di revocare il proprio consenso in merito alla ricezione delle email stesse. La revoca/annullamento delle email (Opt-Out / Unsubscribe) deve generalmente essere facilmente attuabile dal destinatario, ovvero senza l'utilizzo dei dati di accesso (es. login o password).
- L'intestazione e l'oggetto dell'email non devono nascondere o occultare né il mittente né la natura commerciale dell'email. Con occultato o nascosto, si intende il caso in cui l'intestazione o l'oggetto siano creati in modo tale che il destinatario non riceva o riceva informazioni fuorvianti circa l'identità del destinatario o la natura commerciale del messaggio, prima di leggere il contenuto del messaggio stesso.

Configurazione tecnica

- Gli indirizzi del mittente devono essere registrati e fanno parte dell'amministrazione del servizio. L'indirizzo del mittente deve essere abilitato a ricevere email (record DNS MX valido). Il dominio del mittente deve anche avere un Record A di DNS valido. Indirizzi role-based (per esempio abuse@ o postmaster@) non sono consentiti.
- Il cliente dovrà immediatamente eliminare gli indirizzi e-mail delle rispettive mailing list qualora, al momento della consegna, vengano rilevati indirizzi non esistenti e, al più tardi, qualora si siano verificati tre hard bounce. Il tasso totale di hard bounce per ISP normalmente non dovrebbe superare l'1,0%. Gli indirizzi dei destinatari role-based saranno scartati (es. postmaster@, abuse@).
- Il cliente dovrà eliminare gli indirizzi email dalle rispettive mailing list qualora il destinatario classifichi l'email come spam e sporga un reclamo o revochi il consenso a ricevere email.
- Per gli indirizzi "MAIL FROM" inclusi nelle comunicazioni SMTP tra i server email, deve essere inserito un record SPF-From, permettendo dunque lo svolgimento di Test SPF da parte del destinatario. Il record SPF deve finire con -all" o "~all". Qualora le voci necessarie non siano

implementate da parte del cliente entro dieci (10) giorni lavorativi, il nuovo controllo verrà addebitato.

- Il cliente dovrà sempre utilizzare la procedura DKIM (DomainKeys Identified Mail). Per ciascun indirizzo mittente registrato per il cliente presso Retarus, il cliente dovrà fornire una chiave DKIM nel proprio DNS. Qualora le voci necessarie non siano implementate da parte del cliente entro dieci (10) giorni lavorativi, il nuovo controllo verrà addebitato.
- "List-unsubscribe"-Header o "List-help"- Header (vedi RFC 2369) devono sempre essere inclusi in ciascuna email inviata. "List-unsubscribe"- Header è necessaria per le mailing list e deve essere inserita congiuntamente a un "POST HTTPS"-link, unito a una funzione "One-click unsubscribe" (RFC 8058). Il link fornito deve tradursi in una cancellazione diretta tramite clic, almeno a livello della lista. Il mittente può inviare all'utente una conferma di avvenuta cancellazione. Per tutte le altre email, "List-help"- Header deve essere aggiunta al posto della "List-unsubscribe"- Header. "List help"- Header deve includere almeno un indirizzo in formato "mail-to" oppure un link HTTPS. Il link HTTP non sono consentiti. L'utilizzo dell'indirizzo "mailto:" e il link HTTPS devono permettere al destinatario di ricevere informazioni in merito alle motivazioni per le quali tale email gli è stata inviata e le ragioni per cui non è possibile la cancellazione dalla mailing list.

- L'utilizzo di „list-unsubscribe-Post“-Header necessita di un indirizzo URL valido che possa ricevere ed elaborare tali richieste POST.

  Ad esempio:

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

- I link forniti devono attivare un click di iscrizione, almeno a livello della lista. Il cliente inoltre si impegna ad inviare al destinatario un'email che confermi la sottoscrizione.
- Eccezioni a tale obbligo possono essere ammesse qualora non sia possibile annullare l'iscrizione alle e-mail in tal senso, a causa del design del servizio e dell'invio automatico delle e-mail ad esso associato.
- Il Cliente deve impostare un indirizzo e-mail di abuso per la segnalazione dell'abuso di indirizzi e-mail per i destinatari delle e-mail e monitorarlo. L'indirizzo e-mail di abuso può essere configurato ad esempio come abuse@domain.
- L'invio di e-mail al servizio Retarus Transactional Email deve avvenire tramite Transport Layer Security (TLS - opportunistic/enforced) da parte del cliente, secondo lo stato attuale della tecnica. Retarus utilizza per l'invio delle e-mail al destinatario il Transport Layer Security (TLS) utilizzando gli indirizzi IP CSA.
- Retarus è certificato CSA (Certified Senders Alliance). Gli obblighi della collaborazione descritti qui riflettono i requisiti attuali della CSA. La CSA può modificare i propri requisiti in ogni momento. Quindi, il cliente si impegna a osservare qualunque eventuale cambiamento. Il cliente sarà informato di tali modifiche da Retarus.