SaaS Security Solutions for GDPR Compliance:

Trend Micro Email Security White Paper

September, 2020

This whitepaper has been prepared in consultation with Technology Law Firm, Fieldfisher.

It is intended to provide helpful and informative material but should not be relied upon as constituting legal advice on the part of Trend Micro or Fieldfisher. You should always seek your own, independent legal advice where necessary.

Trend Micro SaaS Security Solutions for GDPR Compliance:

Trend Micro Email Security White Paper

Introduction

As a leader in security, Trend Micro has always taken data privacy and protection very seriously. Trend Micro operates in over 50 countries around the world and it works diligently to ensure compliance with regional data protection regulations. Trend Micro solutions are also used by organizations around the world - including Trend Micro's own infrastructure - to protect sensitive user and corporate information from the escalating number and sophistication of attacks happening today.

Trend Micro™ Email Security, a software-as-a-service (SaaS) offering, provides a blend of cross-generational threat techniques to stop all types of email threat.

This white paper outlines how Trend Micro Email Security can be used to help with our customers' compliance with the EU General Data Protection Regulation (GDPR) and how it should be used in a compliant manner with the GDPR. The document also details how Email Security itself adheres to the GDPR principles.

The GDPR

The GDPR took effect throughout the European Union on 25 May 2018. It changes the privacy and security landscape not only in the EU but also globally, as it seeks to extend its extra-territorial reach outside the EU.

The GDPR regulates the "processing" of "personal data":

- "Processing" means any activities performed on personal data and includes storing or receiving personal data, such as, in emails identifying security threats.
- "Personal data" means any information relating to an identified or identifiable living individual, such as contact information.

  Note: "personal data" is much wider than the US concept of "PII" or "personally identifiable information". Data that would not be considered PII could be considered personal data, such as IP addresses or device identifiers.

The GDPR applies to both:

- **controllers**, who decide the "why and how" of processing personal data; and
- **processors**, who are engaged by controllers to host, analyze or process personal data for them.

Under the GDPR:

- **Security** – organizations must implement appropriate technical and organizational measures to protect personal data, including appropriate security measures. Breach of these security requirements could subject controllers to regulatory fines of up to 4% of total annual turnover or (if higher) €20 million, and for processors, up to 2% of total annual turnover or (if higher) €10 million.

- **Data protection by design and by default** – controllers must build data protection, including security, both when designing and implementing their systems and processes and when processing personal data. Infringement of this requirement could expose the organization to a fine of up to 2% of total annual turnover or (if higher) €10 million.

- **Personal data breach notification** – controllers must notify personal data breaches to regulators without undue delay and within 72 hours where feasible, while processors must notify their controllers without undue delay. Controllers must also notify the affected individuals of "high risk" personal data breaches. Fines for non-notification could reach 2% of total annual turnover or (if higher) €10 million.

State of the art security and the ability to **detect and report on threats** are therefore important factors for data protection under the GDPR.

What is Trend Micro Email Security?

Trend Micro Email Security is a cloud-based email gateway solution that delivers continuously updated protection to stop spam, phishing, ransomware, graymail, and malware before they reach your network.

Using Email Security, mail administrators can set up rules to take actions on email messages based on the threats detected. For example, administrators can remove detected malware from incoming messages before they reach the corporate network or quarantine detected spam and other inappropriate messages. Furthermore, intended message recipients or mail administrators can choose to release or delete the quarantined messages.

How does Trend Micro Email Security work?

Email Security does not require hardware on premises. All scanning is hosted off-site in the cloud. Administrators access the Email Security console using a web browser.

Inbound Message Flow

Email Security will first scan incoming email messages before final delivery to the "example.com" Inbound Server.

The flow of messaging traffic is from the Internet, through Email Security, and then to the "example.com" Inbound Server, or local MTA.

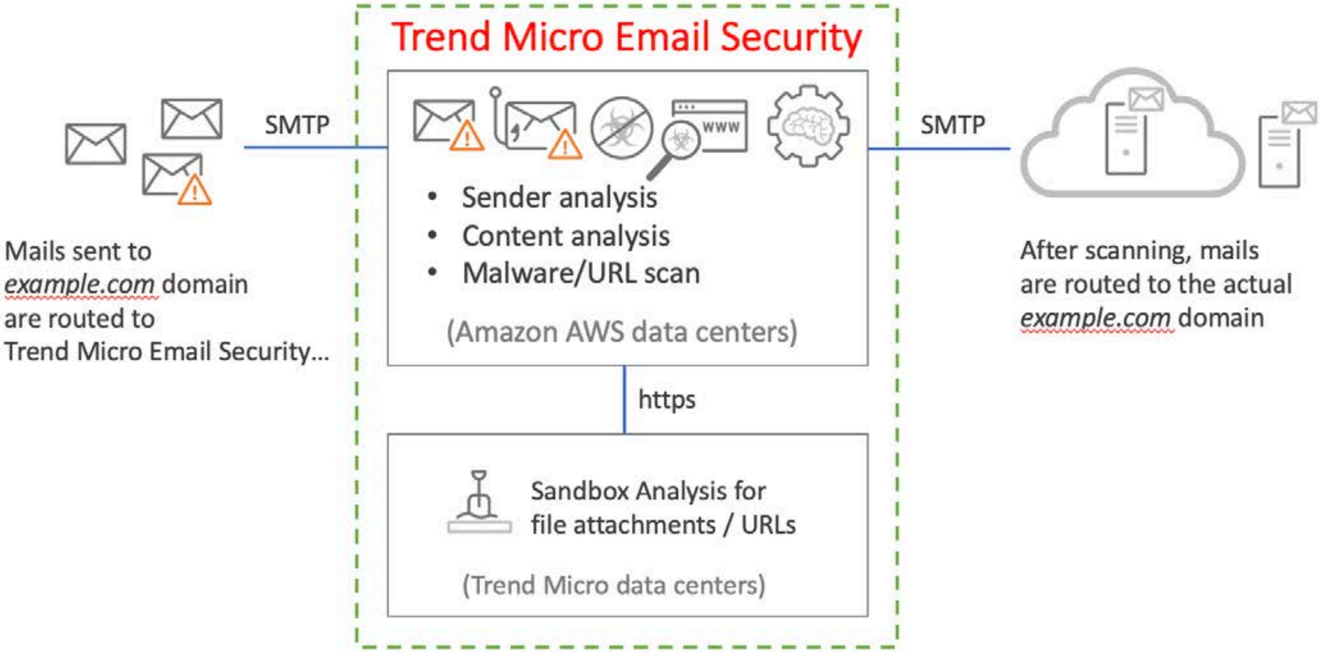
Trend Micro Email Security
SMTP
SMTP
Sender analysis
Content analysis
Malware/URL scan
(Amazon AWS data centers)
https
Sandbox Analysis for file attachments / URLs
(Trend Micro data centers)
Mails sent to example.com domain are routed to Trend Micro Email Security...
After scanning, mails are routed to the actual example.com domain

Figure 1: Trend Micro Email Security Architecture

Evaluation is done in the following order:

- The originating MTA performs a DNS lookup of the MX record for "example.com" to determine the location of the "example.com" domain.
- The MX record for "example.com" points to the IP address of Email Security instead of the original "example.com" Inbound Server.
- The originating MTA routes messages to Email Security.
- Email Security accepts the connection from the originating mail server.
- Email Security performs connection-based filtering at the MTA connection level to decide on an action to take. Actions include the following:
    - Email Security terminates the connection, rejecting the messages.
    - Email Security accepts the messages and filters them using content-based policy filtering.
- Email Security examines the message contents to determine whether the message contains malware such as a virus, or if it is spam, and so on.
- Assuming that a message is slated for delivery according to the domain policy rules, Email Security routes the message to the original "example.com" Inbound Server.

Outbound Message Protection

Email Security scans outgoing email messages before delivery if outbound filtering is enabled. Email Security applies the following policy rules for filtering:

- Spam and phishing
- Malware (viruses, spyware, and so on)
- Web and email reputation
- Data Loss Prevention (DLP)
- Transport Layer Security (TLS) check
- Domain Keys Identified Mail (DKIM) signing

In addition, policy-based encryption is available to secure email messages. Email Security evaluates outgoing messages against regulatory compliance templates defined in DLP policies to prevent data loss by blocking or encrypting messages based on content scanning.

Spam and Phishing Protection

- Email Security protects email users from spam, phishing, Business Email Compromise (BEC), ransomware, and other high-profile attacks.
- The advanced spam protection uses proven Trend Micro anti-spam technologies, including spam signatures and heuristic rules to filter email messages, as well as sophisticated artificial intelligence engines to detect advanced attacks.

Malware Scanning

- Filters all known malware leveraging the Trend Micro™ Smart Protection Network™ (SPN), Trend Micro’s cloud-based threat intelligence network.
- If Email Security detects a suspicious or unknown file/email/URL, it will record related information for up to 90 days in a customer accessible MTA log, securely hosted on Amazon AWS (for further details, please see Appendix 1).
- Multiple state-of-the-art security engines (including pre-execution machine learning) are used to assess the risk of the detected file, and then isolate if appropriate.

Cloud Sandbox (for Trend Micro Email Security Advanced version only)

- If the product is unsure about any email/file/URL, it will be uploaded (via HTTPS) and securely analyzed in a cloud sandboxing service hosted in an ISO 27001 certified Trend Micro-owned data center at DCS-MUC1 in Germany.

- Using advanced techniques like machine learning and behavioral analysis, the cloud sandbox analyzes against multiple operating systems in parallel and can even sandbox Macintosh and Android files.

- To ensure the malware detonates in the sandbox, the product uses industry-leading anti-evasion techniques such as mouse movements and accelerated time environments.

- Customers can configure Email Security to use or not use the cloud sandbox. Suspicious emails/files/URLs are sent to the sandbox only if the customer has configured this.

- Only Trend Micro service personnel can access the sandbox infrastructure, customers have no access to it.

- All evaluated files and emails are securely deleted from the sandbox upon evaluation completion. For details of sandbox logs, please see Appendix 1.

Data Loss Prevention (DLP)

- Allows the customer to identify sensitive information that requires protection, create policies that limit or prevent the transmission of digital assets, and enforce compliance to established privacy standards.

- More than 240 global out-of-the-box templates are included to help with regulatory compliance.

Email Encryption

- Email Security includes the option to encrypt messages using Identity Based Encryption (IBE).
- Email encryption is based on policies, which can include, specific senders or recipients of the message (for example, a rule that encrypts all emails sent from Human Resources or the Legal department), specific content in the message body (i.e. “confidential”), and sensitive data contained in the message (i.e. a DLP template). Trend Micro manages the encryption keys and recipients can read the encrypted message in a modern web browser.

Trend Micro Email Security Communication and Data Access

Emails sent and received are transmitted to Email Security via SMTP. Generally, communications between Email Security and other internal (including, Predictive Machine Learning, Web Reputation Services (WRS) and Email Reputation Services (ERS) and external components are achieved via HTTPS connections.

Many messages are rejected before they are scanned based on the reputation of the IP that is attempting to send the message.

If a message is scanned, Email Security only temporarily stores the customer's transmitted data during scanning, in the application's memory, and subsequently deletes it from memory. By default, Email Security does not store or archive email messages; all messages are processed and immediately passed through to the customer's MTA or inbound server.

Email Security would only store messages for a longer period if the message needs to be quarantined (see below) or if the customer's MTA becomes unavailable. If the customer's MTA becomes unavailable for whatever reason, the customer's message stream is automatically queued for up to ten days or, if less, until such time that the customer's server comes back online.

During the period when the customer’s MTA is unavailable and messages are queued up at Trend Micro’s MTA, Email Security Advanced customers have the option to enable Email Continuity, which allows end users to access the queued emails. Once the customer’s MTA becomes available again, the queued messages are delivered and no longer kept on Trend Micro Email Security MTA.

Data in the course of being scanned cannot be accessed, even by Trend Micro administrators or customer administrators.

Caches

- Email Security creates file scan caches to record file scanning results, storing locally in the geographical region of the service installation. Only the Email Security application can access the cache. Each cache is deleted within 24 hours.

Intercepted items

- On filtering emails, Email Security can take a number of actions based on its own checks (which includes using information from Trend Micro's SPN) and using customer policy rules.

- If a message triggers a content-based policy rule with an "Intercept" action i.e. a risk is detected and for example, the policy action set by the customer is "Change recipient", Email Security will change the recipient of the message and deliver.

- If the customer has enabled the cloud sandbox, Email Security will take temporary quarantine actions for suspicious emails messages. After they have been analyzed, the mail or file will be delivered to the customer's inbound server if there is no detected issue/risk.

- If the next action is to "quarantine" an email message, quarantined items are stored within Email Security for a maximum of 30 days in a transformed format, which is restorable to its original content. After that period, the data will be purged permanently.

- Data retention periods in Email Security are:

Type	Timeframe
Dashboard - Daily data	3 months
Dashboard –Yearly data	2 years
Quarantined emails	30 days
Message queue when customer MTA is unavailable	Incoming: 10 days Outgoing: 1 day

- The customer's administrator can access information about the quarantined items via the quarantine audit information in the administrator console, where they can review and choose to deliver or delete these items to any end user. If EUQ Digest mail is enabled, an end user may also access their own quarantine area, review and take action as an administrator.
- Trend Micro cannot access quarantined items but may have visibility of the quarantine audit information if the customer has a troubleshooting issue, as part of Trend Micro's access to audit information, see below.

Web and Email Reputation

- The web and email reputation services use the SPN to determine whether URLs or IP addresses are malicious. Information is sent in anonymized or pseudonymized form.

Time-of-click protection

- The URL Click Tracking screen enables you to track the URL clicks where Email Security provides Time-of-Click Protection.
- Email Security maintains up to 30 days of URL click tracking log information.
- The URL Click Tracking screen provides the following search criteria:
    - **Dates:** The time range for your query.
    - **Direction:** The direction of messages.
    - **Recipient:** The recipient email address.
    - **Sender:** The sender email address.
    - **URL:** The URL contained in the message**.**
    - **Message ID:** A unique identifier for the message.
- In addition to the search criteria mentioned above, the following URL click tracking information is displayed:
    - **Time of Click:** The time a URL was clicked.
    - **Action Applied:** The action taken on the URL.

System data

- Only Trend Micro's Email Security operations team have access to the Email Security's system and data, which is protected with 2-factor authentication.
- "System data" comprises MTA log, detection log (scanner), UI log and audit log.
- In addition, access to the customer's Email Security configuration information is only authorized after obtaining explicit customer consent to help troubleshoot an issue.
- Customer administrators can view all access logging data by viewing the administration and user events log.

Audit information

- A range of audit information is maintained by Email Security including:

    - quarantined items, see above;
    - mail tracking which allows the customer to investigate the status of an email. By completing a search, the customer can view blocked traffic, accepted traffic and unresolved traffic, which includes, BEC information for email messages detected as analyzed or probable BEC attacks;
    - policy events which allow the customer to identify the type of threat (ransomware,

  - malware, data loss prevention etc.);
  - URL click tracking which enables the customer to track URL clicks where Email Security provides time-of-click protection; and
  - administration and user events, which document how access to the system or data has occurred in Email Security.
- The audit information is stored securely in Email Security and made available to the customer for access over HTTPS to authorized administrators of the customers, with 2-factor authentication (and, if authorized by customers, to the Email Security operations team for troubleshooting). Please see Appendix 1 for more details about audit information including retention periods.

What personal data may be involved when using Trend Micro Email Security, and how?

Scanned emails may contain "personal data", both in their content and in their metadata (to, from, subject, source IP address), and in any attachments.

In order to use the service, customers must provide Email Security with certain information, which likely contains or constitutes personal data. Some examples include: individual employee names and email addresses which may be used to define high profile groups (users that may be frequently forged or spoofed) and specific Email Security policies for enforcement, and as part of a directory import. The customer may also input domain name and incoming mail server IP address information to manage domains on Email Security.

The audit information created by Email Security may also contain personal data. Examples include email sender/recipient email addresses, subject title, IP address and attachment names (names of files attached to scanned emails).

Data processing roles

The customer is the controller, and Trend Micro is the processor, of personal data processed using Email Security.

Email Security scans emails messages on behalf of customers to assist them with the enhancement of their security. The reason why the customer is acting as controller is because they retain full control over what the service can access and how; the personal data processed by Trend Micro in or from Email Security is strictly performed in accordance with the instructions the customer provides using the service system settings. For example, the customer decides which of its employees can access the Email Security console as administrators or otherwise; it can choose which domains are activated and managed; and it determines what rules and policies to apply, including how the service enforces policies for specific users or groups. The customer can also enable or disable:

- Meta information stored in logs.
- Sending suspicious files to the cloud sandbox.
- Machine learning feedback to Trend Micro about suspicious files (disabled by default) to improve its detection capabilities. All files are subsequently deleted.
- Sending data collected with Trend Micro's Anti-Spam Engine to help detect spam, protect users from BEC attacks and graymail, and detect phishing and other attacks.
- Querying the reputation of IP addresses from which emails are sent to/from the customer.
- Querying the reputation of URLs from which emails are sent to/from the customer.
- Re-writing URLs during scanning of the email message body sent to the customer.

The only feature that the customer cannot disable is Trend Micro’s business analytics feedback. Information sent includes customer internet domain, activation code and customer ID/UUID, seats licenses purchased, whether email encryption is enabled/disabled and customer's MX record status.

See the Trend Micro Email Security Data Collection Notice for further details about the Email Security features which collect and transmit data and how the customer can control these features: https://success.trendmicro.com/solution/1120463.

Trend Micro's role

As a processor for customers, Trend Micro is required by the GDPR to maintain appropriate security for the personal data processed for its customers. Trend Micro has other obligations, such as, including certain minimum terms in customer contracts, and in relation to the use of subcontractors/subprocessors.

Security

Trend Micro maintains strong physical, organizational and technical security measures, and ensures segregation and isolation of different customers' data:

- Email Security is certified as ISO 27001:2013 compliant.
- The Email Security team undertakes daily scans of the service to identify any vulnerable components and install updates. Members of the team are also oncall 24x7 to respond to alarms sent by the system.
- Trend Micro’s global InfoSec team also conducts system scans for every major release.
- Email Security uses Amazon S3 for log and QT storage. Amazon S3 is designed for 99.999999999% (11 9’s) of data durability as it automatically creates and stores copies of all S3 objects across multiple systems, so no additional data backup is performed.
- If the primary Email Security site is not available, the traffic will be redirected to a backup site to continue processing. Once the primary site is recovered, traffic is redirected and all data collected in the backup site will be replicated back to primary site.
- The primary Email Security site is hosted on AWS. Certifications and security for their platform are relevant and available at https://aws.amazon.com/compliance/
- All Trend Micro system components hosted outside of AWS are hosted in ISO 27001 certified data centers.
- The encryption keys used to protect outbound email encryption are stored in highly secure data centers in the UK and Germany (ISO 27002 certified). Additionally, the AES-256bit encryption keys and data are separate from one another at all times, preventing the email encryption key service from accessing the data Email Security encrypts or decrypts in outbound or inbound mail.
- All Trend Micro administrators who work with Email Security are Trend Micro employees, who have signed confidentiality agreements as a part of their employment contracts. For more information about employees' screening and security awareness, see https://www.trendmicro.com/en_us/about/legal/product-certifications.html.

Contract terms

- Trend Micro offers customers GDPR terms as a standard part of doing business, see https://www.trendmicro.com/en_us/about/legal.html. Trend Micro also has a process for implementing GDPR terms with relevant subcontractors.

Deletion of data

- Logs are automatically deleted after the retention periods detailed in Appendix 1 at which point, all log data will be purged and cannot be retrieved. Please see Appendix 1 for more information.
- Where messages are scanned and Email Security stores the message because either the customer's MTA is unavailable or a "quarantine" action is taken, such messages are respectively automatically deleted once the Customer's MTA becomes available again or after 10 days.
- If a customer terminates their Email Security account or their license expires, the database schema that contains their account information (and all the customer's account data) is subsequently deleted as part of Trend Micro's maintenance operations and will be deleted 90 days after the license has expired or account termination.
- A customer can remove domain and domain-related data from Email Security by simply deleting it and can submit a case to Email Security to delete account related data.

Breach management

- Although Trend Micro has designed Email Security not to collect personal data, if a personal data breach does happen, Trend Micro has a breach reporting plan to notify customers as necessary to meet breach reporting obligations under the GDPR, and has also implemented 24x7 monitoring and incident response.

How can a customer use Trend Micro Email Security compliantly with the GDPR?

The customer, as the controller, remains responsible for its obligations under the GDPR in relation to the personal data processed in Email Security.

This includes:

- having a "legal basis" for the processing activities;
- complying with core GDPR principles;
- meeting transparency requirements incumbent on controllers;
- addressing individuals' requests to exercise their GDPR rights; and
- complying with other obligations under the GDPR regarding security, data protection by design and by default, and international transfers.

Establishing a legal basis for using Trend Micro Email Security

Personal data cannot be processed without a recognized legal basis. Article 6 of the GDPR recognizes several legal bases, one of which is legitimate interests (Article 6(1)(f)): "the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child".

Furthermore, Recital 49 of the GDPR explicitly acknowledges that the processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring **network and information security**, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, constitutes a legitimate interest of the controller concerned. It cites as examples preventing unauthorized access to electronic communications networks, malicious code distribution and stopping ‘denial of service’ attacks and damage to computer and electronic communication systems.

In addition, EU privacy regulators have also noted, in a pre-GDPR opinion that still largely holds true today, that legitimate interests can extend to processing for physical security, IT and network security purposes (WP217 http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf).

However, regulators (WP217) expect a "balancing test" to be conducted by the controller, to confirm that the processing is indeed necessary and proportionate for that legitimate interest, and is not overridden by individuals' rights (i.e. not too privacy-intrusive). In this day and age, scanning emails/files through services such as Email Security is necessary, given the prevalent and increasing use of email as a vector for threats. The UK Information Commissioner has provided a "legitimate interests assessment" sample template at https://ico.org.uk/media/for-organisations/forms/2258435/gdpr-guidance-legitimate- interests-sample-lia-template.docx, which can be used by customers to perform and document the balancing test. To meet the balancing test, customers should carefully consider the policies, rules and controls they implement when configuring and using Email Security, as well as the scope of their scans, limiting the extent to which their end users are monitored to what is necessary for security purposes and providing appropriate transparency to their end users.

Regulators recommend (WP249 http://ec.europa.eu/newsroom/document.cfm?doc_id=45631) considering mitigating actions to reduce the scale and impact of the scanning on end users, including undertaking a data protection impact assessment (DPIA) and implementing and communicating to end users appropriate monitoring policies as well as privacy notices. In some EU countries, employee works councils may have to be involved in relation to the policies.

Customers should also involve their data protection officer (if appointed) in their legitimate interest assessment and any DPIA.

Email Security has been designed to incorporate safeguards that will assist in any legitimate interest assessment, such as ensuring that logs are only accessible to authenticated individuals over a secure connection and retention is for a defined, relatively short period of time.

Special categories of personal data

For processing "special category" personal data, further conditions beyond legitimate interests must be satisfied. However, EU data protection regulators have acknowledged in an opinion (WP55 http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf), an opinion which has been endorsed by the more recent WP249, that as long as the scanning is not specifically aimed at special category data, they do not consider it unacceptable if in practice it is collected.

Complying with core GDPR principles

The customer is responsible for complying with core principles such as fairness, purpose limitation, data accuracy, and storage limitation/deletion (Article 5 GDPR).

"Integrity and confidentiality" is another core GDPR principle (Article 5(1)(f)), and customers may use a scanning service like Email Security to help meet their obligation to protect the integrity and confidentiality of the personal data of which they are controller.

Transparency and privacy notices

Transparency is also a core GDPR principle and controllers are specifically required to give privacy notices to individuals with certain minimum information.

Customers may comply with this requirement by giving their end users notice of the automated scanning of emails/files/URLs via Email Security, such as through implementing and communicating a monitoring policy.

Individuals' rights

As Email Security only scans emails/files/URLs and temporarily stores the customer's transmitted data during scanning which is then immediately deleted once appropriate action has been taken, the customer retains the original emails/files/URLs including any personal data, and accordingly can deal with individuals' requests to exercise their rights in relation to that data.

Where an email is modified, quarantined, temporarily quarantined or deleted by the service, this is strictly in accordance with the policy rules set by the customer. The customer would determine the rules for deletion (i.e. set its policy of whether to quarantine or delete) and should ensure it is for security purposes and not for avoiding a right of access.

Security and data protection by design and by default

Given the prevalence of email/files/URLs as a threat vector, use of Email Security as a state-of- the-art security tool will assist customers to comply with their security and data protection by design and by default obligations under the GDPR.

Further, the customer can set policy actions for Email Security to encrypt outbound email messages to transfer sensitive information safely.

For more information about some of Trend Micro's own security measures, including our ISO 27001 certification, please see https://www.trendmicro.com/en_us/about/legal/product-certifications.html

International transfers

- **Hosting:** EU customers are hosted in AWS'[1] Frankfurt data center with backup in AWS Ireland, ANZ customers are hosted in AWS Sydney data center, Japan customers are hosted in the AWS Tokyo data center, US and all other customers are hosted in the AWS North Virginia data center, with backup in AWS Ohio. For sandbox capabilities, Japan customers are routed to the AWS Tokyo data center, while all other customers are routed to Trend Micro's German data center.

- **Trend Micro team:** Service operation and InfoSec team members who provide support and troubleshooting are Trend Micro employees. Team members are based in Taiwan and the Philippines.

Trend Micro relies on EU Commission approved model clauses to transfer personal data out of the EEA.

---

[1] The contracts with AWS are held by Trend Micro Taiwan.

Additional Resources

- More information on how Trend Micro can help with GDPR compliance: https://www.trendmicro.com/en_gb/business/capabilities/solutions-for/gdpr-compliance.html
- Information about Trend Micro's GDPR compliance journey: https://www.trendmicro.com/en_us/business/capabilities/solutions-for/gdpr-compliance/our-journey.html
- More information on Trend Micro Email Security: https://www.trendmicro.com/en_us/business/products/user-protection/sps/email-and-collaboration/email-security.html
- More information on other Trend Micro services and products including the Smart Protection Network (SPN): https://www.trendmicro.com/en_us/about/legal/privacy-whitepapers.html

□

- Trend Micro Email Security Data Collection Notice: https://success.trendmicro.com/solution/1120463
- Information on Trend Micro’s product and service approach to data collection: https://success.trendmicro.com/data-collection-disclosure
- Trend Micro data privacy policies: https://www.trendmicro.com/privacy

Appendix 1: Audit information

Log Type	Information Stored	Where Stored (location of log hosting)	Retention Period	Who Can Access
MTA	Email senders, email recipients, Relay MTA, Message ID, suspicious file/URL information	EU customers - EU Japan customers – Japan ANZ customers – Sidney Rest of world customers – US	Automatic deletion after 90 days	Customer Email Security administrator Trend Micro Operations Team (with customer permission)
UI	Account, domain, operations on UI	EU customers - EU Japan customers – Japan ANZ customers – Sidney Rest of world customers – US	Automatic deletion after 30 days	Customer Email Security administrator Trend Micro Operations Team (with customer permission)
Scanner	Email senders, email recipients, email subjects, policy name, policy action	EU customers - EU Japan customers – Japan ANZ customers – Sidney Rest of world customers – US	Automatic deletion after 14 days	Customer Email Security administrator Trend Micro Operations Team (with customer permission)
Audit	Account name, Action and domain	EU customers - EU Japan customers – Japan ANZ customers – Sidney Rest of world customers – US	Automatic deletion after 12 months	Trend Micro Operations Team Customer can only query latest 30 days in admin console
Mail tracking	Email senders Email recipients Email subjects	EU customers - EU Japan customers – Japan ANZ customers – Sidney Rest of world customers – US	Automatic deletion after 90 days	Customer who owns account Trend Micro Operations Team (with customer permission)

Policy events	Email senders Email recipients Email subjects	EU customers - EU Japan customers – Japan ANZ customers – Sidney Rest of world customers – US	Automatic deletion after 30 days	Customer who owns account
URL Click tracking	Email senders Email recipients URL contained in the message	EU customers - EU Japan customers – Japan ANZ customers – Sidney Rest of world customers – US	Automatic deletion after 30 days	Trend Micro Operations Team
Sandbox	Suspicious files, including executables, office/PDF documents, flash, images, HTML, scripts etc.	Japan customers – AWS Japan Rest of world customers - Trend Micro Data Center: MUC1 in Germany	Automatic deletion after 2 days	Cloud Sandbox Operations and Advanced Persistent Threat Teams
System Quarantine	Email	EU customers - EU Japan customers – Japan ANZ customers – Sidney Rest of world customers – US	Automatic deletion after 30 days	Customer who owns account