TREND MICRO

fieldfisher

SaaS Security Solutions for GDPR Compliance:

Trend Micro Cloud App Security White Paper

July, 2019

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:

Cloud App 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.

This white paper explains how Trend Micro™ Cloud App Security, a software-as-a-service (SaaS) offering designed to detect and stop malicious emails and files from impacting an organization, can help with compliance with the EU General Data Protection Regulation (GDPR), as well as improve security posture. This paper also outlines how you can use Cloud App Security compliantly with the GDPR and how the service 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, and scanning emails for 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 in the EU, 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 Cloud App Security?

Cloud App Security enables you to embrace the efficiency of cloud services while maintaining security. It uses state-of-the-art capabilities to protect incoming and internal Microsoft Office 365 email from advanced malware and other threats, and can also help with compliance on other cloud file-sharing services, including Box, Dropbox, Google Drive, SharePoint® Online, and OneDrive® for Business.

Cloud App Security integrates directly with Office 365 and other services using standard APIs, maintaining all user functionality without rerouting email traffic or setting up a web proxy.

According to the Trend Micro Cloud App Security Report 2019 (https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/trend-micro-cloud-app-security-report-2019), the solution was able to detect and block **8.9 million high-risk email threats** missed by Office 365 security. Those threats include over 1 million pieces of malware, 7.7 million phishing attempts, and 103,955 Business Email Compromise (BEC) attacks.

How does Cloud App Security work?

As it is a SaaS offering, Cloud App Security is configured and managed through a secure web console. It accesses emails or files via APIs using a native integration approach (ex: service account for Office 365, access token for Dropbox), performing security scanning in memory without storing any emails or files.

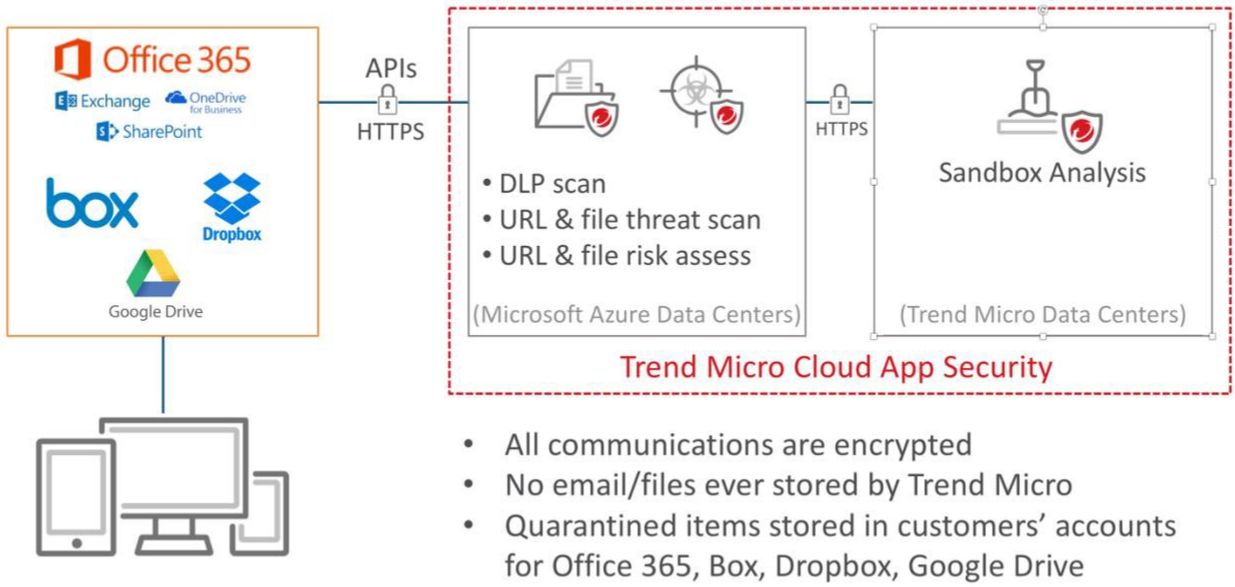
Office 365
Exchange
OneDrive for Business
SharePoint
box
Dropbox
Google Drive
APIs
HTTPS
• DLP scan
• URL & file threat scan
• URL & file risk assess
(Microsoft Azure Data Centers)
HTTPS
Sandbox Analysis
(Trend Micro Data Centers)
Trend Micro Cloud App Security
• All communications are encrypted
• No email/files ever stored by Trend Micro
• Quarantined items stored in customers' accounts for Office 365, Box, Dropbox, Google Drive

Figure 1: Trend Micro Cloud App Security Architecture

Cloud App Security performs real-time scans and on-demand (manual) scans. When it detects malicious or undesirable content (in an email or a file), it automatically takes action according to scanning rules configured by the administrator. Real-time scanning and on-demand scanning apply Advanced Threat Protection and Data Loss Prevention (DLP) policies. The on-demand scan is a unique and powerful feature provided for administrators to perform threat discovery, risk assessment and gain visibility into confidential data usage.

Leveraging XGen™ security and a cross-generational blend of advanced threat techniques, Cloud App Security delivers malware scanning, a cloud sandbox, advanced spam protection, and DLP capabilities.

Malware Scanning

- Filters all known malware leveraging the Trend Micro™ Smart Protection Network™ (SPN), Trend Micro's cloud-based threat intelligence network.

- If Cloud App Security detects a suspicious or unknown file/email attachment, it will record related information for up to 90 days in a customer-only accessible system scan log, securely hosted on Microsoft Azure (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

- If the product is unsure about any file or URL (or both), 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.

- Using advanced techniques like machine learning and behavioural analysis, the cloud sandbox analyzes potential threats against multiple operating systems in parallel andcan 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 Cloud App Security to use or not use the cloud sandbox. Suspicious emails/files/URLs are only sent to the sandbox if the customer has configured this.

- Only Trend Micro service personnel canaccess 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.

Advanced Spam Protection

- Cloud App Security can be configured to deliver advanced spam protection as a complement to email gateway protection services, to further protect Exchange Online users from Business Email Compromise (BEC), ransomware, advanced phishing, and other high-profileattacks.

- 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 (AI) engines to detect advanced attacks.

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.

Cloud App Security Communication and Data Access

The customer's new emails and new or modified files (for non-email scanning, i.e. scanning of files not attached to emails but stored in the customer's cloud storage/application) are transmitted to Cloud App Security. All communications between Cloud App Security and the customer's cloud service, as well as internally between Trend Micro system components, are via secure HTTPS connections. The Cloud App Security service only temporarily stores the customer's transmitted data during scanning, in the application's memory, and subsequently deletes it from memory. Data in the course of being scanned cannot be accessed, even by Trend Micro or customer administrators.

Caches

- Cloud App Security creates file scan caches to record file scanning results, storing file SHA1, file location, policy SHA1, and scan result as an irreversible hash value, in the same geographical region as the customer. Only the Cloud App Security application can access the cache. Each cache is deleted after 24 hours.

Quarantined items

- Emails and files can be quarantined using Cloud App Security. Quarantined items arestored, within each customer’s own cloud application/service storage.

- If the customer has enabled the virtual analyzer (sandbox), Cloud App Security will take temporary quarantine actions for suspicious emails or files. After they have been analyzed, the mail or file will be restored to the customer's cloud service if there is no detected issue/risk. If risk is detected and the policy action set by the customer is “Quarantine”, Cloud App Security will take quarantine actions for those emails or files:
    - for email quarantine, Cloud App Security will create a hidden folder in the end user’s cloud service mailbox, and move the quarantined mail from inbox to the hidden quarantine folder; and
    - for file quarantine, Cloud App Security will create a hidden folder in the customer’s SharePoint or OneDrive site, and move the quarantined file from its current location to the hidden folder.
- Only the customer’s Cloud App Security administrators can download, restore or delete quarantined items (via the Cloud App Security quarantine log web page – for further details of system quarantine logs, please see Appendix 1). Trend Micro cannot access quarantined items.

System data

- Only Trend Micro service team members have access to the Cloud App Security application's system data, which is protected with 2-factor authentication.
- "System data” comprises Trend Micro's virtual machines, service monitoring data, cloud services, and system resources related to its cloud infrastructure, but it does not include any customer data.
- In addition, access to the customer's Cloud App Security configuration information is only authorized after obtaining explicit customer consent to help troubleshoot an issue.
- Customer administrators can view all access logging data through the Cloud App Security web console (for more information on system scan and system audit logs, please see Appendix 1).

Audit information

- All general audit information, inclusive of data access, is centrally stored for 90 days, accessible over HTTPS to authorized administrators of the customer only (and to Trend Micro administrators, but only if authorized by the customer for troubleshooting).
- The only personal data stored in these logs are the user IDs of the relevant customer administrators used for accessing system information, which are recorded in Cloud App Security audit logs. All service debug logs are stored securely for no more than 30 days (then securely deleted) at an isolated cloud network location that is only accessible over HTTPS by authorized service operation team members for troubleshooting purposes. All scan logs are deleted automatically after 90 days. For quarantine logs, customer administrators may choose to automatically delete them after 30, 60, or 90 days.

In summary, all data transmissions are secured by HTTPS and data access is secured by strong authentication. All data is deleted at specific or policy-defined times (defined by the customer), and also as requested by the customer.

What personal data may be involved when using Cloud App 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, organizations must provide Cloud App Security with information needed to access target scanning environments, such as service account information, the company employees' user account names and group/organization unit names in Box, Dropbox and Google Drive. Individual employee names are used by customers to define specific Cloud App Security policies for enforcement. For the same purpose, the customer may input domain, user, and group information in Windows Azure Active Directory; Exchange Online mailbox information; SharePoint Online site collection information; Exchange user names, SharePoint site lists, OneDrive personal site user names and site information, group names in these services, and Office 365 domain names. Some of this information may constitute or contain personal data. All data is store securely within the Cloud App Security service hosted on Microsoft Azure.

The logging data created by Cloud App Security may also contain personal data. Examples may include email senders, email recipients, email locations (i.e. where the email is stored on the customer's cloud storage/application, such as: employeename@organisationname\Inbox), email subjects, attachment names (names of files attached to scanned emails), file modifiers, file locations (i.e. where the file is stored on the customer's cloud storage/application), and file names. All log data is stored securely, accessed via HTTPS, authenticated with 2-factor authentication, and securely deleted after a maximum of 90 days. Please see Appendix 1 for details.

Data processing roles

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

The service scans emails and files on behalf of customers to assist them with the enhancement their security. The reason why the customer is acting as controller is that they retain full control over what the service can access and how. For example, the customer decides which of its employees can access the Cloud App Security console as administrators or otherwise; it chooses what user names/group names etc. to configure for scanning; 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:

- Mail/file meta information stored in logs
- Scanning of email attachments
- Sending suspicious files and URLs to the cloud sandbox
- Machine learning feedback on email attachments (disabled by default), to enable suspicious files to be sent to a secure cloud sandbox for further analysis. All files are subsequently deleted
- Querying the reputation of IP addresses from which emails are sent to the customer
- Querying the reputation of URLs from which emails are sent to the customer

See the Cloud App Security Data Collection Notice for the full details of the service here: https://success.trendmicro.com/solution/1119582

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:
    - Cloud App Security is certified as ISO 27001:2013 compliant.
    - The Cloud App Security service team undertakes regular scans of the service to identify any vulnerable components and install updates.
    - Trend Micro's global InfoSec team also conducts system scans and there are regular backups to ensure business continuity.
    - As the primary service is hosted on Microsoft Azure, certifications and security for their platform are relevant and available at https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings. All Trend Micro system components hosted outside of Microsoft Azure are hosted in Trend Micro-owned ISO 27001 certified data centers.
    - All Trend Micro administrators who work with Cloud App 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

- If a customer terminates their Cloud App Security account, they can delete all related organizational service data, including policies, quarantined emails and files, and access to any connected service account.

- All domain, user, group information, and the service account will automatically be deleted after a one-month "grace period" following termination. All related service and debug logs that may contain customer-related data will be deleted within the 90 day standard service log deletion time period.

Breach management

- Although Trend Micro has designed Cloud App 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 Cloud App 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 Cloud App 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 Cloud App 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 Cloud App 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 the Trend Micro service, as well as the scope of their scans, limiting the extent to which their employees are monitored to what is necessary for security purposes, providing appropriate transparency to their employees.

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 employees, including undertaking a data protection impact assessment (DPIA) and implementing and communicating to employees 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.

Cloud App 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 Cloud App 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 employees notice of the automated scanning of emails/files via Cloud App Security, such as through implementing and communicating a monitoring policy.

Individuals' rights

As Cloud App Security only takes copies of emails/files and deletes them after use, the customer retains the original emails/files 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 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 as a threat vector, use of Cloud App 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.

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 Microsoft Azure's[1] western Europe data center, with sandbox capabilities hosted in Trend Micro’s German data center.
  - For customers in North America (and multiple other countries using the US service), the primary service components are hosted in Microsoft Azure US west, with sandbox capabilities hosted in Trend Micro's US data center.
  - Japanese customers are hosted in the Microsoft Azure's Japan east data center and also leverage Trend Micro’s US-based data center.
- **Trend Micro team:**
  - Service operation and InfoSec team members who provide support and troubleshooting are Trend Micro employees based in the Philippines.

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

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

Additional Resources

- More information on how Trend Micro can help with GDPR compliance: www.trendmicro.com/gdpr
- 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 Cloud App Security: https://www.trendmicro.com/en_us/business/products/user-protection/sps/email-and-collaboration/cloud-app-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
- Cloud App Security Data Collection Notice: https://success.trendmicro.com/solution/1119582
- Information on Trend Micro's product and service approach to datacollection: 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
System Scan	- Email senders, recipients, locations, & subjects -Attachment names -File modifiers, locations, & names	- EU customers – EU - Japan customers—Japan - Rest of world customers—US	Automatic deletion after 90 days.	Only customer's Cloud App Security administrator
System Quarantine	- Email senders, recipients, locations, & subjects -Attachment names -File modifiers, locations, & names	- EU customers – EU - Japan customers—Japan - Rest of world customers—US	Automatic deletion based on customer configured policy of 30, 60, or 90 days.	Only customer's Cloud App Security administrator
General System Audit	- Name of customer's Cloud Application Security Administrator - Administrative Actions such as create or change policy, login, logout. - Administrative Action details	- EU customers – EU - Japan customers—Japan - Rest of world customers—US	Automatic deletion after 90 days.	Only customer's Cloud App Security administrator
Cloud Sandbox	File name and hash value	- EU customers – EU - Japan customers—Japan - Rest of world customers—US	Automatic deletion after 60 days.	Only customer's Cloud App Security administrator
System Debug	System operational information only. No customer data	- EU customers – EU - Japan customers—Japan - Rest of world customers—US	Automatic deletion after 30 days.	Cloud App Security operations team