TREND MICRO

fieldfisher

SaaS Security Solutions for GDPR Compliance:

Trend Micro Worry-Free Business Services 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:

Worry-Free Business Security Services 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™ Worry-Free Business Security Services (Worry-Free), a software-as-a-service (SaaS) offering for small businesses, protects multiple Windows computers, Macs and Android Devices located in or out of the office, from viruses and other threats from the web.

This white paper outlines how Worry-Free 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 Worry-Free 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 Worry-Free?

Worry-Free is an integrated solution, consisting of the Security Agent that resides at the endpoint and the Worry-Free Server that manages all Security Agents. Unique Web Threat Protection stops threats before they reach devices and inflict damage or steal data. This safer, smarter, simpler protection from web threats will not cause devices to slow down. You can centrally manage security from anywhere without the need to add a server, install server software, configure settings, or maintain updates. Trend Micro security experts host and constantly update the service infrastructure as a part of the SaaS offering.

Worry-Free is powered by the Trend Micro™ Smart Protection Network™ (SPN), a next generation cloud- client infrastructure that delivers security which is smarter than conventional approaches. Unique in-the- cloud technology combined with Worry-Free's lighter-weight Security Agent delivers rapid response updates to endpoints when a new threat is detected, enabling faster time-to-protection, reducing the spread of malware, reliance on conventional pattern downloads, and eliminates the delays commonly associated with desktop updates.

How does Worry-Free work?

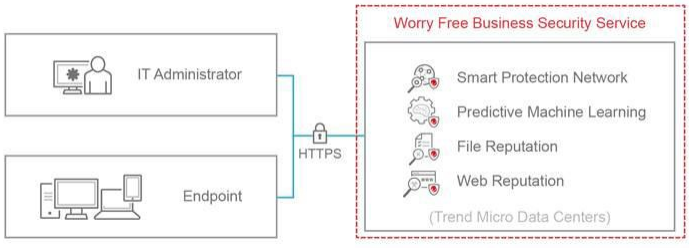

Figure 1: Trend Micro's Worry-Free architecture

Worry-Free consists of the following components:

- *Web console:* manages all Agents from a single location.
- *Worry-Free Server:* hosts the service including the web console; collects and stores logs; and helps control virus/malware outbreaks.
- *SmartScan Server:* enables scanning of clients using pattern files, reducing the overall load on the client.
- *Security Agent:* a small program installed on the Windows endpoints that protects the endpoints from virus/malware, spyware/grayware, Trojans, and other web threats.
- *Security Agent for Mac:* a small program installed on the Mac endpoints that protects the endpoints from virus/malware, spyware/grayware, Trojans, and other web threats.
- *Security Agent for Android:* a small app installed on Android devices that protects the device from unsafe websites, malicious apps, and provides anti-theft features.
- *Security Profile for iOS:* a profile installed on iOS devices that provides anti-theft features.

About the Web Console

As it is a SaaS application, customers can access Worry-Free via the secure web console, which is the central point for monitoring Security Agents on all endpoints. It comes with a set of default settings and values that you can configure based on your security requirements and specifications. The web console uses standard internet technologies, such as Java, CGI, HTML, and HTTPS.

Organizations can use the web console to:

- deploy Agents to endpoints;
- organize Agents into logical groups for simultaneous configuration and management;
- configure product settings and set scan configurations on single or multiple networked endpoints;
- receive notifications and view log reports for threat-related activities; and
- receive notifications and send outbreak alerts through email messages when threats are detected on endpoints.

About the Security Server

At the center of Worry-Free is the Server. The Server hosts the centralized web-based management console for Worry-Free. The Server, along with the Agents, forms a client-server relationship. The Worry-Free Server enables viewing security status information and Agents, configuring system security, and updating Agent components from a centralized location. The Server also contains the database where it stores logs of detected internet threats being reported to it by the Agents.

About the Security Agent

Security Agents report to the server from which they were installed. They send event information such as threat detection, Agent start-up and/or shutdown, start of a scan, and completion of an update to the server in real time.

Administrators control Security Agent settings from the server and can choose to grant users the privilege to configure specific settings and the Security Agents download and install the security settings based on the policy requirements.

Worry-Free delivers the following features:

Application Control	Application Control uses the kernel-level blocking method to block applications before execution on your corporate endpoints. Kernel-level blocking prevents applications from starting by blocking file access. This provides greater security, but may unexpectedly block or momentarily delay access to certain files needed by allowed applications, so configuration care is an important part of deployment.
Behavior Monitoring	Behavior Monitoring constantly monitors endpoints for unusual modifications to the operating system or on installed software by both known and unknown threats.
Damage Cleanup Services	Damage Cleanup Services™ cleans computers of file-based and network viruses, and virus and worm remnants (Trojans, registry entries, viral files) through a fully-automated process. To address the threats and nuisances posed by Trojans, Damage Cleanup Services does the following: • Detects and removes live Trojans • Kills processes that Trojans create • Repairs system files that Trojans modify • Deletes files and applications that Trojans drop Damage Cleanup Services runs automatically in the background so it is not necessary to configure it. Users are not even aware when it runs. However, if required, Worry-Free may notify the user to restart their endpoint to complete the process of removing a Trojan.
Data Loss Prevention	Data Loss Prevention (DLP) safeguards an organization's digital assets against accidental or deliberate leakage. DLP allows administrators to: • Identify the digital assets to protect • Create policies that limit or prevent the transmission of digital assets through common transmission channels, such as email messages and external devices

	• Enforce compliance to established privacy standards
Device Control	Device Control regulates access to external storage devices and network resources connected to computers. Device Control helps prevent data loss and leakage and, combined with file scanning, helps guard against security risks.
Full Disk Encryption	Worry-Free provides you the ability to remotely trigger Microsoft BitLocker Drive Encryption and perform full disk encryption on managed Windows endpoints.
Firewall	The firewall can block or allow certain types of network traffic by creating a barrier between the client and the network. Additionally, the firewall will identify patterns in network packets that may indicate an attack on clients.
Predictive Machine Learning	The Predictive Machine Learning engine can protect your network from new, previously unidentified, or unknown threats through advanced file feature analysis and heuristic process monitoring. Predictive Machine Learning can ascertain the probability that a threat exists in a file and the probable threat type, protecting you from zero-day attacks.
Ransomware Protection	Enhanced scan features can identify and block ransomware programs that target documents which run on endpoints by identifying common behaviors and blocking processes commonly associated with ransomware programs.
Security Risk Protection	Worry-Free protects endpoints from security risks by scanning files and performing a specific action for each security risk detected. Worry-Free uses a “smart scan” to make the scanning process more efficient. This technology works by off-loading a large number of signatures previously stored on the local endpoint to Smart Protection Network resources (may be localized or cloud-based). Using this approach, the system and network impact of the ever-increasing volume of signature updates to endpoint systems is significantly reduced.
Web Reputation	Web Reputation enhances protection against malicious websites. Web Reputation leverages Trend Micro's extensive web security database to check the reputation of URLs that customers are attempting to access or URLs embedded in email messages that are contacting websites.

Worry-Free Communication and Data Access

Customers connect to Worry-Free via HTTPS connections. Generally, communications between Worry-Free and other internal (including, TrendX, Cloud App Security and Hosted Email Security) and external components are achieved via HTTPS connections.

Quarantined items

- URLs, emails and files can be quarantined using Worry-Free. Quarantined items are encrypted and temporarily moved to a quarantine folder in the Security Agent installation folder on the local device. From there, the Security Agent sends the infected file to a central quarantine directory of which, by default, is located on the Security Server (or such other quarantine directory specified by the customer) i.e. within each customer's own cloud application/service storage.

- Quarantined items are stored until deleted by the customer's administrator with access to the local endpoint with administrative privileges.

- The customer administrator can access information about the quarantined items via the system quarantine log in the administrator console, where they can review, delete, or restore quarantined results.

- 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.

System data

- Only Trend Micro's Worry-Free service operations team have access to the Worry-Free system and data, which is protected with strong password-based authentication.

- In addition, access to the customer's Worry-Free console, configuration and server components is only authorized after obtaining explicit customer consent to help troubleshoot an issue.

- Customer administrators can view all access logging data by viewing the system audit log.

Audit information

- Worry-Free keeps comprehensive logs about virus/malware and spyware/grayware incidents and updates categorized under three different log groups.

- All audit information is centrally stored for the retention periods set out in Appendix 1, accessible over HTTPS to customer administrators via the secure web console (and, if authorized by customers, to the Worry-Free service operations team).

- Please see Appendix 1 for more details about audit information including personal data stored and applicable retention periods.

What personal data may be involved when using Worry-Free, and how?

Worry-Free may process personal data in order to perform its functions. Some examples include:

- in order to use the service and set up groups to manage endpoints, customers provide Worry-Free with certain device and account information which likely contains or constitutes personal data such as, IP addresses, user name, host name and mobile number;

- Worry-Free works with Hosted Email Security or Cloud App Security to monitor ransomware attacks on detected email servers and synchronizes data such as, email senders and recipients; and

- customers can collect geo-location data from registered mobile devices to enable administrators to locate devices remotely.

Data processing roles

The customer is the controller, and Trend Micro is the processor, of personal data processed using Worry-Free.

Worry-Free protects endpoints 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 Worry-Free is strictly performed in accordance with the instructions the customer provides using the service system settings and for administrators to identify a specific client that has mitigated threats or do manual follow-up by the customer administrator. For example, the customer decides which of its employees can access the Worry-Free console as administrators or otherwise; it can choose which endpoints to protect; manages its user access permissions; and it determines what rules and policies to apply, including how the service enforces policies for specific users or groups.

You can enable or disable all the Worry-Free service features, which process personal data with the exception of the information collected from endpoints used to identify an endpoint for administrators as part of device management.

See the Worry-Free Data Collection Notice for further details about how the Worry-Free features collect and transmit data and how the customer can control these features: https://success.trendmicro.com/solution/1120515-worry-free-business-security-services-data-collection-notice

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:

- Worry-Free is certified as ISO 27001:2013 compliant.

- The Worry-Free service operation team undertakes bi-weekly scans of the service to identify any vulnerable components and install updates. Members of the time are also on call 24x7 to respond to alarms sent by the system.

- Trend Micro’s global InfoSec team also conducts regular system scans.

- The database on the service is backed up daily and kept for one year.

- If a primary Worry-Free site fails, the service will be redirected to an AWS backup site in either Oregon, Frankfurt or Dusseldorf to continue processing. Once the primary site is recovered, the service is redirected.

- The primary sites are hosted at Trend Micro's data centers DCS-SJC1 and DCS-MUC1. All Trend Micro system components hosted outside of these data centers are hosted in Trend Micro-owned ISO 27001 certified data centers.

- All Trend Micro administrators who work with Worry-Free 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 in the same location the log is stored and cannot be retrieved. Please see Appendix 1 for more information.

- If a customer terminates their Worry-Free 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. Customers have a 30 day grace period following termination or expiry of their license, after this grace period has expired, deletion of data takes place.

- A customer can remove data from Worry-Free by simply deleting it e.g. deleting a user account or deleting a log (or set a log deletion schedule).

Breach management

- Although Trend Micro has designed Worry-Free 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 Worry-Free 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 Worry-Free.

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 Worry-Free

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, security protection services such as Worry-Free is necessary, given the prevalent and increasing complexity and sophistication of different channels for security 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 Worry-Free, as well as the scope of their monitoring and security services, limiting the extent of their processing activities 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.

Worry-Free 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 security service like Worry-Free 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 and non-automated scanning and monitoring via Worry-Free, such as through implementing and communicating a monitoring policy.

Individuals' rights

A customer may receive a request from an individual end user exercising their rights under the GDPR. As Worry-Free only temporarily stores personal data it processes and/or the customer retains the original copy personal data, the customer can accordingly deal with individuals' requests to exercise their rights in relation to that data.

Where an email or file is quarantined, modified 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 security threats, use of Worry-Free 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, please see https://www.trendmicro.com/en_us/about/legal/product-certifications.html

International transfers

- **Hosting:** EU customers are hosted in Trend Micro's data center DCS-MUC1 with back-up stored in AWS'[1] Frankfurt and Dusseldorf data centers and all other customers are hosted in Trend Micro's data center DCS-SJC1 with back-up stored in AWS' US Oregon data center. Sandbox capabilities are hosted in Trend Micro's German data center.

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

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 Worry-Free: https://www.trendmicro.com/en_gb/small-business/worry-free-services.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
- Worry-Free Data Collection Notice: https://success.trendmicro.com/solution/1120515
- 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
Security Risk Detection	Filename, URL, email address	- Rest of world customers - Trend Micro DCS-SJC1 - EU customers – Trend Micro DCS-MUC1 **Back-up:** - Rest of world customers - AWS (US Oregon) - EU customers – AWS (Frankfurt) and (Dusseldorf)	Automatic deletion after 60 days (unless otherwise configured by customer)	Customer administrator and Service operation team
Web (or Management) Console Events	Account name, actions taken	- Rest of world customers - Trend Micro DCS-SJC1 - EU customers – Trend Micro DCS-MUC1 **Back-up:** - Rest of world customers - AWS (US Oregon) - EU customers – AWS (Frankfurt) and (Dusseldorf)	Automatic deletion after 60 days (unless otherwise configured by customer)	Customer administrator and Service operation team
System	Internal system logging from Apache and the core application. Data logged can include internal system administrator account name, UUID & IP.	- Rest of world customers - Trend Micro DCS-SJC1 - EU customers – Trend Micro DCS-MUC1 **Back-up:** - Rest of world customers - AWS (US Oregon) - EU customers – AWS (Frankfurt) and (Dusseldorf)	Automatic deletion after 60 days	Service operation team