SaaS Security Solutions for GDPR Compliance:

Trend Micro Apex One as a Service 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:

Apex One as a Service 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 Apex One™ as a Service (Apex One), a software-as-a-service (SaaS) offering protects endpoints, on or off the corporate network, against malware, Trojans, worms, spyware and ransomware with protection that adapts against new unknown variants as they emerge.

This white paper outlines how Apex One 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 Apex One 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 Apex One as Service?

Apex One provides enhanced security against unknown, zero-day, and web-based threats on top of, and alongside, your current endpoint protection solution.

An integrated solution, Apex One consists of the Security Agent (an installed piece of software) that resides at the endpoint and a hosted server program that manages all Security Agents. The Security Agent guards the endpoint and reports its security status to the server. The server, through the web-based management console, makes it easy to set coordinated security policies and deploy updates to every Security Agent.

Apex One is powered by the Trend Micro™ Smart Protection Network™ (SPN), an advanced cloud-client infrastructure that delivers security which is smarter than conventional approaches. Unique in-the-cloud technology and a lighter-weight Security Agent delivers rapid response updates to endpoints when a new threat is detected. This enables faster time-to-protection, removing the reliance on conventional pattern downloads, and eliminates the delays commonly associated with desktop updates. Apex One customers benefit from increased network bandwidth, reduced processing power requirements, and associated cost savings. Customers also get immediate access to the latest protection wherever they connect - within the company network, from home, or on the go.

How does Apex One as a Service work?

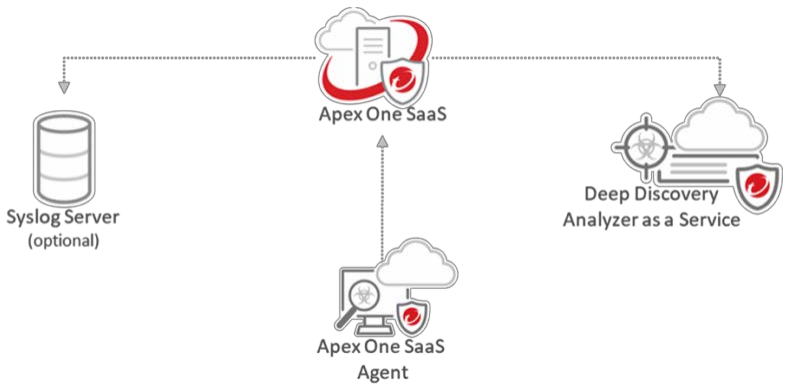

Figure 1: Trend Micro Apex One architecture

Apex One as a Service consists of the following components:

- *Apex Central Server:* manages all Agents from different Trend Micro products from a single location.
- *Apex One Server:* hosts 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.
- *Trend Micro Security Agent:* a small software program installed on the Windows endpoints that protects the endpoints from virus/malware, spyware/grayware, Trojans, and other web threats.
- *Trend Micro Security Agent for Mac:* a small software program installed on the Mac endpoints that protects the endpoints from virus/malware, spyware/grayware, Trojans, and other web threats.
- *Security Agent for Android:* an 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.
- *Optional Sandboxing:* Customers can subscribe to a sandbox as a service option (Deep Discovery Analyzer as a Service) or leverage their own Deep Discovery Analyzer appliance on premise. This optional capability enables Apex One to send suspicious objects to a sandbox for further analysis.

About the Web Console

As it is a SaaS application, customers can access Apex One via secure web console. The web console uses standard internet technologies, such as Java, CGI, HTML, and HTTP.

The web console is the central point for monitoring Security Agents throughout the corporate network. It comes with a set of default settings and values that you can configure based on your security requirements and specifications. 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 the service is the Apex One Server. The Apex One Server hosts the centralized web-based management console for Apex One. The Server, along with the Agents, form a client-server relationship. The Apex One Server enables viewing security status information, viewing 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, Security Agent startup, Security Agent 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.

Apex One as a Service delivers the following features:

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.
Connected Threat Defense	Configure Apex One to subscribe to the Suspicious Object lists from the Apex Central server. Using the Apex Central console, you can create customized actions for objects detected by the Suspicious Object lists to provide custom defense against threats identified by endpoints protected by Trend Micro products specific to your environment. You can configure Security Agents to submit file objects that may contain previously unidentified threats to a sandbox (either a hosted option or a customer's own on-premise device) for further analysis. After assessing the objects, the sandbox adds any objects found to contain unknown threats to the sandbox Suspicious Objects lists and distributes the lists to other Security Agents throughout the network.
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.
Antivirus / Security Risk Protection	Apex One protects computers from security risks by scanning files and then performing a specific action for each security risk detected. An overwhelming number of security risks detected over a short period of time signals an outbreak. To contain outbreaks, Apex One enforces outbreak prevention policies and isolates infected computers until they are completely risk-free. Apex One uses 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 Sources. Using this approach, the system and network impact of the ever-increasing volume of signature updates to endpoint systems is significantly reduced.
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, Apex One may sometimes notify the user to restart their endpoint to complete the process of removing a Trojan.
Web Reputation	Web Reputation technology proactively protects Agent endpoints within or outside the corporate network from malicious and potentially dangerous websites. Web Reputation breaks the infection chain and prevents the downloading of malicious code. Verify the credibility of websites and pages by integrating Apex One with the Trend Micro SPN.
Apex One Firewall	The Apex One Firewall protects endpoints and servers on the network using stateful inspections and high-performance network virus scans. The customer can control traffic access (and block attacks) through the creation of firewall rule actions to filter connections by application, IP address, port number, or protocol, and then apply the rules to different groups of users.
Data Loss Prevention	Data Loss Prevention safeguards an organization's digital assets against accidental or deliberate leakage. Data Loss Prevention 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 endpoints. Device Control helps

	prevent data loss and leakage and, combined with file scanning, helps guard against security risks.
Behavior Monitoring	Behavior Monitoring constantly monitors endpoints for unusual modifications to the operating system or on installed software.
Security solution agnostic	Agents running in "Coexist" mode are compatible on any supported Windows endpoint, running any endpoint security software.

Apex One Communication and Data Access

Customers connect to Apex One via HTTPS connections. Generally, communications between Apex One and other internal and external components are achieved via HTTPS connections.

Quarantined items

- URLs, emails and files can be quarantined using Apex One. Quarantined items are encrypted and temporarily moved to a quarantine folder in the Security Agent installation folder on the endpoint. From there, the Security Agent sends the quarantined items to the designated 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.

- If the customer has subscribed to and enabled the virtual analyzer (a separately licensed sandbox feature), Apex One can also take temporary quarantine actions for suspicious objects (files or URLs). 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”, Apex One will take quarantine actions for those emails or files as set out above.

- Quarantined items are stored for a maximum of 60 days after license expiry and after that period, the data will be purged permanently.

- The customer administrator can access information about the quarantined items via the suspicious objects log in the web console, where they can review and 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 Apex One service operations team have access to the Apex One system and data, which is protected with password-based authentication.

- "System data” comprises data used by Apex One as a Service as a part of ongoing operations designed to detect threats on endpoints and in emails. This includes the logging of data (see Appendix 1).

- In addition, access to the customer's Apex One configuration information is only authorized after obtaining explicit customer consent to help troubleshoot an issue.

- Customer administrators can view all access logging data.

Audit information

- ApexOne keeps comprehensive logs to document information about the service's operations and for the purposes of this whitepaper are categorized into the log types described at Appendix 1.

- 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 Apex One 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 Apex One, and how?

Apex One 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 Apex One with certain device and account information which likely contains or constitutes personal data such as, IP addresses, user name and telephone numbers;

- Active Directory synchronisation allows our customers to map Apex Central's User/Endpoint Directory according to their organizational structure which collects information from a customer's Active Directory such as, telephone numbers, job title, email addresses, user account name etc.; and

- to protect against programs that exhibit malicious behaviour, files for malware detection, or transmission of sensitive information, Apex One may collect IP, URL, username and hostname information from endpoints.

Data processing roles

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

Apex One 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 Apex One is strictly performed in accordance with the instructions the customer provides using the service's system settings. For example, the customer decides which of its employees can access the Apex One 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.

See the Apex One Data Collection Notice for further details about the Apex One features which collect and transmit data and how the customer can control these features: https://success.trendmicro.com/solution/1120644-trend-micro-apex-one-as-a-service-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:

- Trend Micro's global InfoSec team conducts daily vulnerability scanning and Trend Micro schedules monthly maintenance (including bug fixes and security patches) to the service backend.

- Members of the Apex One service operation team are also on call 24x7 to respond to incidents, leveraging the Damage Clean-up Cloud Service Operations Center for monitoring and incident response.

- As the primary site 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 Apex One are Trend Micro employees, who have signed confidentiality agreements as part of their employment contracts. For more information about employee 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.

- If a customer terminates their Apex One 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 60 days after the license has expired or account termination.

- A customer can remove data from Apex One by simply deleting it e.g. deleting a log from the directory or deleting quarantined items.

Breach management

- Although Trend Micro has designed Apex One 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 Apex One 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 Apex One.

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 Apex One

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 Apex One 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 Apex One, 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.

Apex One 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 Apex One 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 Apex One, 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 Apex One 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 Apex One 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 Microsoft Azure's[1] West Europe (Amsterdam) data center with back-up stored in Microsoft Azure's North Europe (Dublin) data center and all other customers are hosted in Microsoft Azure's Central US (IOWA) data center with back-up stored in Microsoft Azure's East US 2 Virginia data center. If a customer subscribes to the sandboxing feature (separately), sandboxes are hosted in Trend Micro's Munich, Germany data center.

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

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

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 Apex One: https://www.trendmicro.com/en_gb/business/products/user-protection/sps/endpoint.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

- Apex One Data Collection Notice: https://success.trendmicro.com/solution/1120644-trend-micro-apex-one-as-a-service-data-collection-notice

- 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

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

Appendix 1: Audit information

Log Type	Information Stored	Where Stored (location of log hosting)	Retention Period	Who Can Access
Virus/Spyware detection Ransomware detection Data loss forensic data	IP, mac address, hostname Hostname, URL Forensic data (includes: email, attached files, message or network transfer data)	Rest of world customers: Microsoft Azure's Central US (IOWA) data center EU customers: Microsoft Azure's West Europe (Amsterdam) data center Back-up: Rest of world customers: Microsoft Azure's East US 2 Virginia data center EU customers: Microsoft Azure's North Europe (Dublin) data center	30 days	Customer administrator and Service operation team
IPortal SSO	Account ID, IP	Rest of world customers: Microsoft Azure's Central US (IOWA) data center EU customers: Microsoft Azure's West Europe (Amsterdam) data center	30 days	Customer administrator and Service operation team

		Back-up: Rest of world customers: Microsoft Azure's East US 2 Virginia data center EU customers: Microsoft Azure's North Europe (Dublin) data center		
Data loss prevention	User name, hostname, IP	Rest of world customers: Microsoft Azure's Central US (IOWA) data center EU customers: Microsoft Azure's West Europe (Amsterdam) data center Back-up: Rest of world customers: Microsoft Azure's East US 2 Virginia data center EU customers: Microsoft Azure's North Europe (Dublin) data center	180 days	Customer administrator and Service operation team
Suspicious object detection	Hostname, IP, file hash	Rest of world customers: Microsoft Azure's Central US (IOWA) data center	90 days	Customer administrator and Service operation team

		EU customers: Microsoft Azure's West Europe (Amsterdam) data center Back-up: Rest of world customers: Microsoft Azure's East US 2 Virginia data center EU customers: Microsoft Azure's North Europe (Dublin) data center		