Trellix Privacy Data Sheet We bring security to life.

Trellix Threat Intelligence Exchange - On Premises (TIE - On-Prem)

The purpose of this Privacy Data Sheet is to provide Customers of Trellix TIE - On-Prem with details on how Trellix captures, processes, and stores[1] telemetry information, including personal data (or personally identifiable information), to help them understand and assess the impact of the telemetry capabilities on their overall privacy posture.

TIE - On-Prem is a solution which protects servers, computer systems, laptops and tablets against known and unknown threats like malware, suspicious communications, unsafe websites and files made available by Trellix to companies or persons who obtain a Trellix TIE - On-Prem subscription.

Trellix will process personal data from TIE - On-Prem in a manner that is consistent with this Privacy Data Sheet. In jurisdictions that distinguish between Data Controllers and Data Processors, Trellix is the Data Controller for the personal data processed to administer and manage the Customer relationship. Trellix is the Data Processor for the personal data processed by TIE - On-Prem to provide its functionality.

Note: This Privacy Data Sheet is a supplement to the Trellix Website Privacy Notice.

Product Overview

Trellix TIE - On-Prem optimizes threat detection and response by narrowing the time gap from initial malware encounter to eventual containment of malware, from days, weeks, and/or months down to milliseconds. TIE - On-Prem rapidly analyzes files and content from several sources within the Customer's environment and automatically makes intelligent, informed security decisions based on file reputation, rules, reputation thresholds and criteria set by Customer security policies.

Trellix TIE - On-Prem combines threat intelligence from global sources such as Trellix Global Threat Intelligence (Trellix GTI) and/or Trellix Intelligence Virtual Execution - Cloud (Trellix IVX - Cloud) with intelligence from local sources. Local sources include collected data from Customer's Trellix ePolicy Orchestrator On Premise (ePO - On-Prem) integration into Customer's network infrastructure, composed of Customer endpoints, gateways, and installed advanced analysis solutions.

[1] In this document, we adopt the broad definition of "processing" that appears at Article 4(2) of the GDPR: "'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means …", which includes, but is not limited to the following non-exhaustive series of examples: "collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

TIE - On-Prem includes Trellix Endpoint Security's Adaptive Threat Protection module (ATP) that allows Customers to create policies for blocking and allowing files based on reputation, where TIE - On-Prem processes information about file and certificate reputations, then passes that information to other endpoints within the Customer network infrastructure.

Thus, TIE - On-Prem acts as a reputation broker, providing real-time reputation information to enable automatic and adaptive detection and response. Using Trellix Data Exchange Layer (Trellix DXL), Trellix TIE - On-Prem instantly shares collective intelligence across Customer's security ecosystem, allowing multiple Trellix security solutions and integrations to operate symbiotically and simultaneously to enhance protection throughout the Customer network infrastructure.

Trellix TIE - On-Prem includes the following security features:

- Rapid-detection and response protection against security threats and malware;
- Allowlisting and blocking specific files and certificates based on reputation and Customer risk criteria;
- Real-time integration with Trellix Intelligent Sandbox (Trellix TIS), Trellix Intelligent Virtual Execution (Trellix IVX), Intelligent Virtual Execution Cloud (Trellix IVX - Cloud) and Trellix Global Threat Intelligence (Trellix GTI) to provide detailed assessments and additional data on malware classification;
- Integration with Trellix Endpoint Security (Trellix ENS) Web Control and Trellix Intrusion Prevention System, which increases end-to end protection and detection capabilities;
- Integration with Trellix Enterprise Security Manager (Trellix ESM) to create reports of files and certificates while monitoring file and certificate events;
- Integration with Trellix GTI's private cloud for consuming reputations that come from a single-tenant and dedicated private setup instead of Trellix GTI's public cloud;
- Integration with Trellix Application Control (Trellix ACC) to work with Trellix TIE server and Trellix GTI server.

Please see, Trellix Threat Intelligence Exchange for additional information.

Please also see, Trellix ePolicy Orchestrator On-Prem, Trellix Endpoint Security, Trellix Global Threat Intelligence, Trellix IVX Cloud, Trellix Enterprise Security Manager, and Trellix Application and Change Control - On-Prem for additional information.

Trellix TIE - On-Prem can be implemented as one of two deployment options:

- **Trellix TIE - On-Prem via ePolicy Orchestrator on Premise (ePO On - Prem) standalone deployment** - Customers use tenant credentials (Trellix Agent) for ePO On - Prem to create/deploy, manage, and enforce security policies; or,
- **Trellix TIE - On-Prem via ePolicy Orchestrator on Premise (ePO On - Prem) virtual deployment** - Customers manage the deployment via their hosted VM Ware ESXi, Nutanix, or Amazon Web Services (AWS) regional clouds. Customers use tenant credentials (Trellix Agent) for ePO On - Prem to create/deploy, manage, and enforce security policies.

Personal Data Processing

Trellix TIE - On-Prem intelligently manages multiple devices and systems concurrently, so that security information is shared across the Customer's network infrastructure. TIE - On-Prem manages remote servers, endpoint devices, managed nodes, and network appliances and enables automated threat detection and response, performed in concert with other Trellix security products and services.

TIE - On-Prem captures data to perform automatic monitoring and detection of cybersecurity vulnerabilities across the entire Customer network infrastructure. Trellix TIE On-Prem utilizes theTrellix DXL framework to pass reputation information on to the ePO - On-Prem service. Trellix ePO On Prem in turn shares automated threat-detection information, based on Customer policy, configuration and available local and global intelligence, with other Customer subscribed Trellix security products and/or services.

Based on Customer requirements and network configuration, a Customer may decide to enable TIE - On-Prem's sandboxing feature to bolster automated threat-detection and response to determine malicious behavior. TIE - On-Prem's sandboxing feature is only available if TIE-On Prem is integrated with Trellix Intelligent Sandbox (TIS), Trellix Intelligent Virtual Execution (IVX), or Trellix Intelligent Virtual Execution - Cloud (IVX - Cloud).

- **Trellix TIE - On-Prem via ePolicy Orchestrator on Premises (ePO On - Prem) standalone and virtual deployments** - Captured event information is sent automatically by Trellix Agent through the Trellix Data Exchange Layer (DXL) using TLS version 1.2 encryption to Trellix Threat Intelligence Exchange (TIE) server/database within the Customer's network infrastructure.

As a result, Trellix TIE - On-Prem may process a range of data potentially containing personal information. The table below shows the data processed by TIE - On-Prem to provide its services and describes why the data is processed.

Table 1. Personal Data Processed by Trellix Threat Intelligence Exchange - On-Premises

Personal Data Category	Types of Personal Data Processed	Purpose of Processing
Administrative Data	General Identification Information: ● Trellix Agent GUID ● First Name ● Last Name ● Email Address of ePO Admin ● ePO Admin User ID ● Registered Server Credentials (if using Registered Servers feature) ● Company Billing Address ● Active Directory Username (optional configuration through if enabled by ePO Admin) ● Machine Name	To access TIE services for SecOps operations ensuring compliance, providing reporting, and facilitating troubleshooting.

	• Mac Address • IP Address • Timestamps • AD Username (if enabled)	
Generated Data	Executed File Samples (only when the sandboxing feature is enabled by a Customer): • Hashed File Reputation Information • NDI Hash • File Names • File URL	Used for threat detection, system communication and system management.
Collected Data	Configuration Information: • Server Tasks: ○ Database Cleanup	Used for product troubleshooting. File reputation information is used to calculate local prevalence of executed files for improved threat detection.

***Please note the Personal Data Categories explained below and used throughout Privacy Data Sheets for Trellix products and/or services:**

Administrative Data: Information to enable the service and/or manage the Customer relationship;

Generated Data: Information generated by the product (events, evidence, logs);

Collected Data: Information generated by the Customer (policies and configurations).

Data Center Locations

Trellix TIE - On-Prem data center locations vary depending on the Customer's deployment model and use of subscribed optional features.

For standalone implementation - the data center is located within the Customer's network infrastructure.

Table 2. Data Center Locations

Data Center Provider	Data Center Location
Not Applicable	**Not Applicable**

Trellix TIE - On-Prem with Global Threat Intelligence enabled (Private Cloud) - the data center is located within the Customer's network infrastructure.

Table 2a. Data Center Locations

Data Center Provider	Data Center Location
Not Applicable	**Not Applicable**

Trellix TIE - On-Prem with Global Threat Intelligence (GTI) enabled (Public Cloud) - Trellix uses its own data centers as well as third-party infrastructure providers to deliver the service globally. Trellix GTI processes the personal data in Trellix's instance in Amazon Web Services, Inc. (AWS) datacenters located in the United States, the United Kingdom, Brazil, Germany, India, Japan, and Singapore. Trellix's regional clouds provide options to address Customers' data location preference. Customers have the choice to select a region or to default to their nearest region for data processing. This means that, unless otherwise modified by a system administrator, the traffic in certain countries will be directed to a defined compute location.

Table 2b. Data Center Locations

Data Center Provider	Data Center Location
AWS	AWS US East (Virginia)
AWS	AWS US West (Oregon)
AWS	AWS US West (Northern California)
AWS	AWS US East (Ohio)
AWS	AWS US East (Northern Virginia)
AWS	AWS Brazil (Sao Paulo)
AWS	AWS United Kingdom (London)
AWS	AWS Germany (Frankfurt)
AWS	AWS India (Mumbai)
AWS	AWS Japan (Tokyo)
AWS	AWS Singapore

Trellix TIE - On-Prem with Sandboxing via Trellix Intelligent Virtual Execution On-Prem (IVX - On-Prem) enabled - the data center is located within the Customer's network infrastructure.

Table 2c. Data Center Locations

Data Center Provider	Data Center Location
Not Applicable	**Not Applicable**

Trellix TIE - On-Prem with Sandboxing via Trellix Intelligent Virtual Execution - Cloud (IVX - Cloud) enabled - Trellix uses its own data centers as well as third-party infrastructure providers to deliver the service globally. IVX - Cloud processes the personal data in Trellix's instance in Amazon Web Services, Inc. (AWS) regional clouds located in the United States and Germany. By default, Customers are directed to the nearest available regional data center where the service is deployed . This means that the traffic in certain countries will be directed to a defined compute location in the United States or Germany.

Table 2d. Data Center Locations

Data Center Provider	Data Center Location
AWS	AWS US East (Virginia)

AWS	Germany (Frankfurt)

Subprocessors

Trellix partners with service providers that act as subprocessors for the TIE - On-Prem service and contracts to provide the same level of data protection and information security that you can expect from Trellix. A current list of subprocessors for the service is below:

Table 3. Subprocessors

Subprocessor	Personal Data Category	Service Type	Location of Data Center
AWS	Generated Data	Hosting	AWS East (Virginia)
AWS	Generated Data	Hosting	Germany (Frankfurt)
AWS	Collected Data	Hosting	AWS US West (Oregon)
AWS	Collected Data	Hosting	AWS US West (Northern California)
AWS	Collected Data	Hosting	AWS US East (Ohio)
AWS	Collected Data	Hosting	AWS US East (Northern Virginia)
AWS	Collected Data	Hosting	AWS Brazil (Sao Paulo)
AWS	Collected Data	Hosting	AWS United Kingdom (London)
AWS	Collected Data	Hosting	AWS Germany (Frankfurt)
AWS	Collected Data	Hosting	Mumbai
AWS	Collected Data	Hosting	Tokyo
AWS	Collected Data	Hosting	AWS Singapore
OKTA	Administrative Data	Authentication	AWS West (Oregon)

Cross-Border Data Transfer

In the event of a need to share personal information with Trellix personnel in regions outside of those identified in the Data Center Locations section above, we will do so in compliance with applicable requirements for transfer of personal data, including those of the EU Standard Contractual Clauses as approved by the European Commission and/or other legal instruments recognized by EU data protection laws. For a more detailed assessment of our international data transfers, please refer to the Trellix Transfer Impact Assessment statement.

Access Control

Access to Customer information is subject to Trellix's Access Management Policy. Access is protected by multiple authentication and authorization mechanisms. Trellix has an account administration application that provides a central access point to request and perform administrative functions for account requests across multiple platforms. All resources have an owner who is responsible for deciding who will

be granted access to that resource. Privileged access to resources is restricted to authorized users with a business need, consistent with the concepts of least privilege and segregation of duties based on roles and job functions. Shared accounts are prohibited. All usernames are traceable to a specific human user. User access credentials are promptly removed when user access is no longer authorized (e.g., Trellix employment terminates).

Remote user access by Trellix personnel is performed through a secure virtual private network (VPN) connection that requires multi-factor authentication (MFA). If remote access to production resources is required outside the VPN, then a TLS encrypted connection and MFA are required.

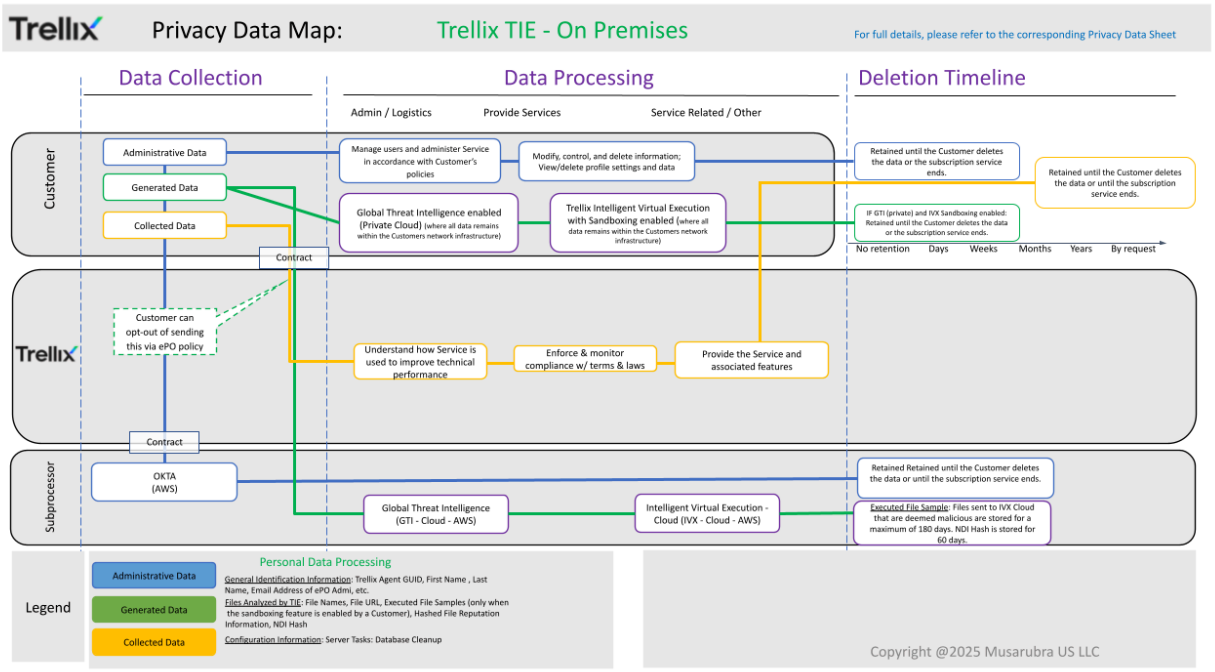
The table below lists the personal data used by TIE - On-Prem to carry out the service, who can access that data, and why.

Table 4. Access Control

Personal Data Category	Who has access	Purpose of the access
Administrative Data	Customer	To identify systems and observe executed files.
	Trellix	To troubleshoot Customer issues as needed.
Generated Data	Customer	To provide details and analysis of executed files.
	Trellix	To troubleshoot Customer issues as needed.
Collected Data	Customer	To provide details and analysis of executed files.
	Trellix	For threat detection efficacy.

Trellix Threat Intelligence Exchange - On-Premise Data Flow Diagram

The key data flows associated with the information processing activities described in this document are shown below.



Customer Privacy Options

Trellix designs its products to support our Customers' compliance with global data protection and compliance obligations. It does this by addressing threat intelligence and security challenges at the application, network, and endpoint levels, and in the cloud. In addition, Trellix offers product features that help our Customers meet their EU General Data Protection Regulation (GDPR) and other legal compliance goals. Such features include, but are not limited to data localization options, policy enforcement, access controls, logging capabilities, individual rights processing, and cross-border data transfer mechanisms.

Customers control whether the TIE - On-Prem product is enabled or disabled. When it is disabled, no data processed by the service is collected and sent to the Cloud and no data is downloaded by the product from the cloud data centers.

Data Portability

Except with respect to Registration Information, the Customer can forward the personal data processed by TIE - On-Prem to a third-party data store. If applicable, to effectuate data portability, Customers may request assistance from Trellix Engineering for a large-scale movement of data (e.g., Customer does not renew subscription and asks for all data to be transferred to a third-party data store).

Data Deletion and Retention

The table below lists the personal data used by TIE - On-Prem, the length of time that data needs to be retained and why we retain it.

A data subject may request deletion of his or her Personal Data by sending a data subject request as described below in this Privacy Data Sheet.

A Customer may request data deletion by submitting a ticket to Trellix support at newcase@mail.thrive.trellix.com. When a Customer makes a request for deletion, Trellix will purge the requested data from its systems to the extent required by applicable law and may retain administrative data required for legitimate business purposes (e.g., billing records).

Table 5. Data Retention

Personal Data Category	Retention Period	Reason for Retention
Administrative Data	Retained until the Customer deletes the data or until the subscription service ends.	Reporting, providing the service, and troubleshooting
Generated Data	Retained until the Customer deletes the data or until the subscription service ends. Executed File Sample (only when the sandboxing feature is enabled by a Customer): ● Files sent to IVX Cloud that are deemed malicious are stored for a maximum of 180 days. ● NDI Hash is stored for 60 days.	Reporting, providing the service, and troubleshooting. Analysis and research.
Collected Data	Retained until the Customer deletes the data or until the subscription service ends.	Analysis and research.

Personal Data Security

Files stored on or processed by Trellix's systems are secured with state-of-the-art technologies, and Trellix implements rigorous technical and organizational security controls designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

Table 6. Personal Data Security

Personal Data Category	Type of Personal Data	Security Controls and Measures
Administrative Data	See Table 1	Encrypted at rest

Generated Data	See Table 1	Encrypted in transit and at rest
Collected Data	See Table 1	Encrypted in transit and at rest

*Additional details for product certifications are available upon request.

Compliance with Privacy Requirements

Trellix is committed to protecting personal data processed in the global and regional Trellix GTI and Trellix IVX-Cloud clouds. We will not access the content of files in a way in which we could learn meaningful information about natural persons, other than in exceptional cases where it is necessary for identifying security threats.

The Privacy Office and Trellix Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Trellix products and services. The Service is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements.

Further, in addition to complying with our stringent internal standards, Trellix also maintains third-party validations to demonstrate our commitment to information security.

Exercising Data Subject Rights

Users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, or deletion of the personal data processed by the Service.

We will confirm identification (typically with the email address associated with a Trellix account) before responding to the request. If we cannot comply with the request, we will provide an explanation. Please note, users whose employer is the Customer/Controller may be redirected to their employer for a response.

Requests can be made by submitting a request via:

1) the Trellix Individual Data Request Form

2) by postal mail:

In the U.S. by registered mail:
Musarubra US LLC
Attn: Legal Department –Privacy
2611 Internet Blvd, Suite 200,

Frisco, TX 75034

or call us at +1 (214) 494-9190

In the European Economic Area by registered post:
Musarubra Ireland Limited
Attn: Legal Department –Privacy
Building 2000, City Gate

Mahon, Cork, Ireland

or call us at +353 21 467 2000

In Japan by registered mail:
Musarubra Japan KK
Attn: Legal Department –Privacy
Shibuya Mark City West

1-12-1 Dogenzaka, Shibuya-ku, Tokyo 150-0043

About This Privacy Data Sheet

Trellix Privacy Data Sheets are reviewed and updated on an annual, or as needed, basis.

Please note that the information provided with this document concerning technical or professional subject matter is for general awareness only, may be subject to change, and does not constitute legal or professional advice, warranty of fitness for a particular purpose, or compliance with applicable laws.