Trellix Privacy Data Sheet We bring security to life.

Trellix Native Drive Encryption On - Premises (TNE - On-prem)

The purpose of this Privacy Data Sheet is to provide Customers of Trellix TNE - 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.

Trellix TNE- 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's TNE - On-prem subscription.

Trellix will process personal data from Trellix TNE - 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 Trellix TNE - On-Prem to provide its functionality.

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

Product Overview

Trellix TNE - On-prem is a solution that allows Security Operations Administrators (SecOps Admins) using Trellix ePolicy Orchestrator - On-Premises (ePO - On-prem) to automatically and proactively manage Apple® FileVault and Microsoft® BitLocker, which provides full-disk encryption on Macintosh (Mac) and Microsoft Windows systems.

Trellix TNE - On-prem protects data on devices that are lost or stolen and deployed through the ePO - On-Prem console. With Trellix TNE - On-prem, SecOps Admins can manage encryption keys and pin features on devices within the Customer's network infrastructure. The TNE - On-prem service provides components that are installed on the Customer's Trellix ePO - On-prem server, and on all Microsoft Windows and Mac endpoints within the Customer's network infrastructure.

[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."

With Trellix TNE - On-prem, SecOps Admins can perform core functions from ePO - On-prem's command center including:

- Proactive management of Apple® FileVault and Microsoft® BitLocker;
- Report encryption status; and
- Import, store, and retrieve recovery keys.

Adopting TNE - On-prem for BitLocker means that Customers no longer need to license, manage, or maintain Microsoft BitLocker Administration and Monitoring (MBAM) or its associated servers. The Customer's SecOps Admin can consolidate servers and eliminate the related Microsoft licenses, providing significant cost savings and reduced management overhead.

Trellix TNE - On-prem ensures that Customers have consistent enforcement of enterprise-wide policy enforcement and compliance across your encryption technology stack. Customers can also use the report-only feature of TNE - On-prem without having to actively manage FileVault or BitLocker. Trellix TNE - On-prem provides comprehensive reports that give Customers complete visibility of their organization's encryption status. Report queries can also be used as a dashboard monitor that automatically updates every five (5) minutes.

Data Protection Self Service Portal (DPSSP) is an optional companion ePO extension that can be used with TNE - On-prem. DPSSP allows Customers' ePO SecOps Admins to set up a web portal for users to retrieve recovery keys to unlock their systems where log on has failed, without the need to contact support directly.

Trellix TNE - On-prem includes two product extensions and a client package:

- The TNE - On-prem software packages are installed on the Customer's systems and apply the policies received from the Customer's ePO - On-prem server.
- Customer SecOps Admin extensions are installed on Customer's ePO - On-prem service. This extension allows you to manage and report on both FileVault and BitLocker on Customer systems by deploying the relevant policy to the system.
- The optional DPSSP extension is a separate extension that integrates with ePO On-Prem to provide self-recovery capabilities for client users.

Trellix TNE - On-prem is offered as:

- **Standalone deployment:** Available to install by the Customer's SecOps Admin to configure settings through the interface.

Please see Trellix Data Encryption for additional information related to the Trellix Native Data Encryption solution.

Please also see Trellix ePolicy Orchestrator On Premise (ePO - On-Prem) Privacy Data Sheets for additional information.

Personal Data Processing

Trellix Native Drive Encryption is a management product that allows Trellix ePO - On-Prem SecOps Admins to use the data processed by e-PO On-Prem to manage Apple FileVault and Microsoft BitLocker. Apple FileVault and Microsoft BitLocker products provide full disk encryption on Macintosh (Mac) and Windows systems, respectively. To initiate the service, the Customer's SecOps Admins configure Trellix ePO - On-prem policies, run Trellix ePO - On-prem queries and reports, and check the status of Trellix ePO - On-prem managed endpoints.

To activate TNE-On-prem, the Customer's SecOps Admin installs TNE - On-prem extensions in the Trellix ePO - On-prem server. Once the TNE - On-prem software is loaded, TNE - On-prem packages are deployed throughout the Customer's network infrastructure. Finally, TNE - On-prem is then installed and activated on all endpoints within the Customer's network infrastructure, whereby Customer policies are automatically assigned.

After successful TNE - On-prem activation, all endpoints are protected by Apple® FileVault and Microsoft® BitLocker, according to the applied policies. Note that, Trellix may capture information differently depending on the TNE deployment version:

- **Standalone deployment**: In standalone deployments, the TNE - On-prem solution reads data stored on the Customer's network infrastructure endpoints and no data is ever captured by Trellix.

As a result, Trellix TNE - On-prem may process a range of data potentially containing personal information. The table below shows the personal data processed by TNE - On-prem to provide its service and describes why the data are processed.

Table 1. Personal Data Processed by Trellix Native Drive Encryption on Premises

Personal Data Category	Types of Personal Data Processed	Purpose of Processing
Administrative Data	General identification information: ● User Name ● User ID ● User SID ● UserDN ● LdapDN ● AD Password	Required for product functionality, diagnostics, and for audit entries.
Generated Data	Incidents / Events: ● Threat Events ● Recovery Key Path (on error) Evidence: ● Not Applicable	Required for product functionality and diagnostics.
Collected Data	Configuration Information: ● Machine Name	Required for product functionality and diagnostics.

	• ePO Leaf Node ID • System ID • Group ID • Group Name • Policy Name • Policy ID • Domain User Names • User Names • Volume Properties • Domain Password • Agent GUID • Recovery Key IDs • Trellix Agent IP Address • Trellix Agent Host Name • System Name IP Address • Volume Name • Serial Number	

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

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**

Subprocessors

Trellix partners with service providers that act as subprocessors for the Trellix TNE - 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 TNE - On-prem is below:

Table 3. Subprocessors

Subprocessor	Personal Data Categories	Service Type	Location of Data Center

Not Applicable	**Not Applicable**	**Not Applicable**	**Not Applicable**

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 Trellix TNE - On-prem to carry out the service, who can access that data, and why.

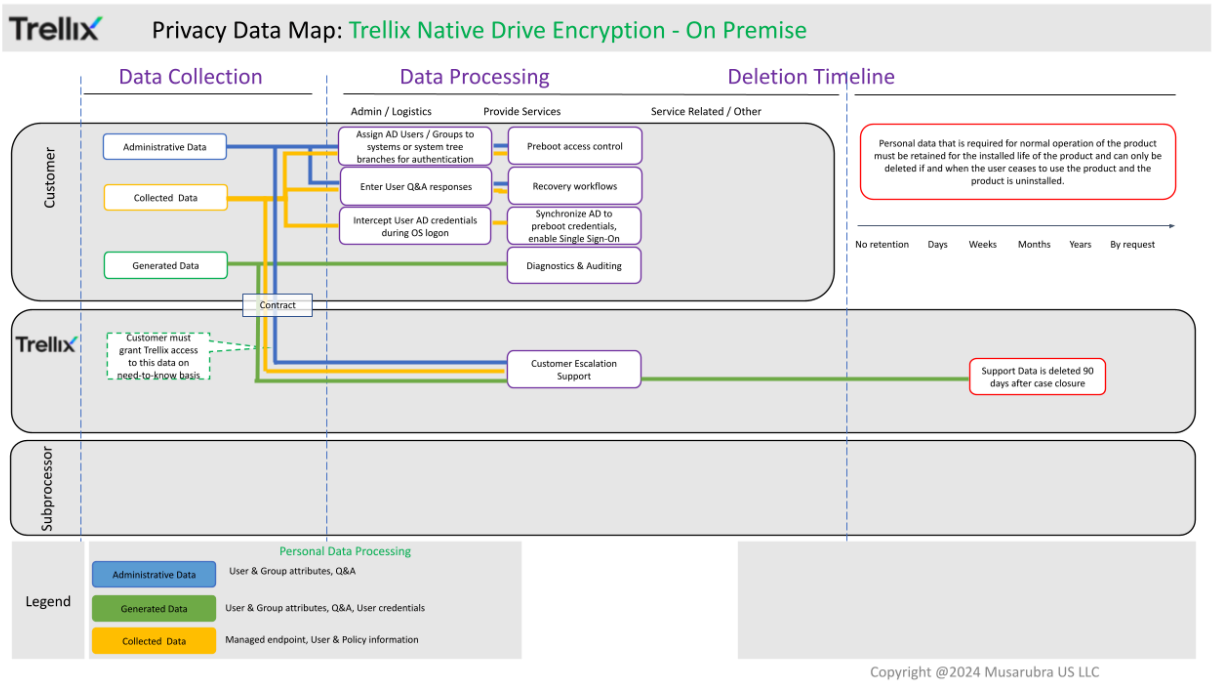
Table 4. Access Control

Personal Data Category	Who has access	Purpose of the access
Administrative Data	Customer	Required for product functionality. Access is limited to the Customer's SecOps Admins in accordance with Customer policies and controls.
	Trellix	Debugging of Customer/operational data in the event of an escalation.
Generated Data	Customer	Required for product functionality and diagnostics.

	Trellix	Debugging of Customer/operational data in the event of an escalation.
Collected Data	Customer	Required for product functionality. Access is limited to the Customer's SecOps Admins in accordance with Customer policies and controls.
	Trellix	Required for product functionality and diagnostics.

Trellix Native Drive Encryption 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 TNE - On-prem service 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 service from the cloud data centers.

Data Portability

Except with respect to Registration Information, the Customer can forward the personal data processed by TNE - 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 TNE - 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 support_reply@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	Not Applicable.	Not Applicable.
Generated Data	Data submitted to Trellix for the purpose of troubleshooting during a support case is retained for 90 days.	To analyze a support case.
Collected Data	Not Applicable.	Not Applicable.

Personal Data Security

Files stored on or processed by Trellix's systems are secured with state-of-the-art technologies, and Trellix operates 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 in transit *
Generated Data	See Table 1	Encrypted in transit
Collected Data	See Table 1	Encrypted in transit

* Sensitive data such as cryptographic key material is also encrypted at rest.

**Additionally, details for product certifications are available upon request.

Compliance with Privacy Requirements

Trellix is committed to protecting personal data processed in global and regional 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
6000 Headquarters Drive, Suite 600

Plano, Texas, 75024

or call us at +1 (888) 847-8766

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, Chibuyaku, 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.