
Trellix Wise™ for Private Cloud

The purpose of this Privacy Data Sheet is to provide Customers of Trellix Wise™ for Private Cloud with details on how Trellix captures, processes, and stores¹ 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 Wise™ for Private Cloud is the core of an agentic Security Operations Center (SOC) that deploys and operates fully within the Customer's environment, including fully air-gapped networks. Trellix Wise™ for Private Cloud focuses on investigation, threat hunting, and remediation, capable of operating 24/7. It is provided to companies or persons who obtain a Trellix Wise™ for Private Cloud subscription.

Trellix will process personal data from Trellix Wise™ for Private Cloud 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 Wise™ for Private Cloud to provide its functionality.

Note: This Privacy Data Sheet is a supplement to the [Trellix Website Privacy Notice](#).

Product Overview

Modern adversaries utilize Artificial Intelligence (AI) to operate at machine speed, presenting challenges for traditional, human-only security operations teams. Historically, mitigating this gap required transmitting sensitive security data to the cloud, incurring unpredictable usage costs while attempting to address an expanding threat landscape.

To address these challenges, Trellix offers Trellix Wise™ for Private Cloud, which serves as the core of a Customer's agentic SOC. It can be deployed on-premises, within fully air-gapped networks, or inside a private cloud. With Trellix Wise™ for Private Cloud, every model, knowledge graph, learned context, and stage of reasoning executes locally, ensuring that telemetry, evidence, and institutional knowledge remain entirely within the Customer's environment.

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."

Three core agents (Investigation, Remediation, and Hunting) work around the clock to support SOC teams and investigate 100% of alerts, respond within human-defined guardrails and human-in-the-loop approvals, and proactively hunt stealthy threats. Designed as an always-on first responder, the Wise Investigation Agent automatically evaluates, correlates, and triages every incoming alert in minutes rather than hours or days. It learns the Customer's unique operational workflows by ingesting local context, user roles, and maintenance patterns to identify real threats against false positives.

When the Investigation Agent confirms a Wise investigation, the Remediation Agent takes action after inheriting the full evidence chain, mapped blast radius, and entities in scope, then translates them into a governed response plan for the Customer to control, scoped to Customer security team permissions.

The Hunting Agent proactively identifies threats by continuously applying threat intelligence across telemetry. It transforms threat hunting from a specialized, periodic activity into a continuous discipline across the Customer's environment. When always-on hunting is enabled, the agent operates continuously within the parameters and guardrails defined by the Customer.

Trellix Wise™ for Private Cloud uses open-weight Large Language Models (LLMs) that execute locally. To address specialized SOC applications, local models are enhanced using Retrieval-Augmented Generation (RAG) and domain-specific fine-tuning techniques. Customer telemetry is never used to train or retain foundational models.

Trellix Wise™ for Private Cloud is designed for on-premises deployment, supporting environments with strict data residency, regulatory, or air-gapped requirements.

Trellix Wise™ for Private Cloud includes the following security features:

- Autonomous investigation of security alerts;
- Confidence-scored, white-box verdicts with MITRE ATT&CK mapping, auditable by both the SOC team and compliance/audit stakeholders;
- Bring-Your-Own-Hardware (BYOH) deployment on infrastructure the Customer already controls.

Trellix Wise™ for Private Cloud can be implemented as:

- **Virtual deployment of Trellix Wise™ for Private Cloud** - Customers manage the deployment via their hosted VMware ESXi, Linux KVM, Windows Hyper-V, Amazon Web Services (AWS), Microsoft Azure or Google Cloud Platform (GCP) instance.

Personal Data Processing

Rather than forcing a data migration, Trellix Wise™ for Private Cloud connects directly to a Customer's existing SIEMs, data lakes, and other third-party tools, enriching alerts with organizational context and structuring raw telemetry into localized knowledge graphs. Security analysts benefit from seamless alert ingestion and centralized analysis of finished investigation reports, complete with verdicts and confidence scores. These integrations enable the solution to ingest alerts, enrich investigations with context, and export results to connected platforms.

The foundational control is locality. In on-premises, air-gapped and private cloud deployments, all processing — models, knowledge graphs, learned context, vector stores, and enrichment — executes entirely within the Customer's environment. Personal data contained in alerts, investigation evidence, and directory content is never required to leave the Customer's environment for Trellix Wise™ for Private Cloud to function.

Trellix Wise™ for Private Cloud includes optional integration with Trellix Threat Intelligence services, providing Customers with the latest intelligence on advanced cyber attacks. With Trellix Wise™ for Private Cloud, Customers may access Trellix Threat Intelligence based on the data sharing license they choose, including an offline license, a restricted one-way license, or a connected two-way license.

With an offline license, Customers import Trellix Threat Intelligence updates through air-gapped transfer mechanisms and no data is captured by Trellix Wise™ for Private Cloud.

With a restricted one-way license, Customers automatically receive the latest Trellix Threat Intelligence and security content updates, and no data is captured by Trellix Wise™ for Private Cloud.

With a connected two-way license, Customers automatically receive the latest Trellix Threat Intelligence and security content updates. This license type also allows Customers to share telemetry regarding bug reports, threats, and malware identified within their environment back to Trellix to enhance detection efficacy, where the uploaded threat metadata is anonymized.

Thus, Trellix will capture information differently depending on the Trellix Wise™ for Private Cloud deployment version:

- **Virtual deployment of Trellix Wise™ for Private Cloud (offline license and restricted one-way license):** The solution reads data stored within the Customer's network environment and no data is captured by Trellix Wise™ for Private Cloud.
- **Virtual deployment of Trellix Wise™ for Private Cloud (for connected two-way license):** Information is encrypted at rest using FIPS-validated AES-256 and in transit using TLS 1.2 or higher.

Trellix Wise™ for Private Cloud may process a range of data potentially containing personal information. The table below shows the personal data processed by Trellix Wise™ for Private Cloud to provide its services and describes why the data is processed.

Table 1. Personal Data Processed by Trellix Wise™ for Private Cloud

Personal Data Category	Types of Personal Data Processed	Purpose of Processing
Administrative Data	<u>General Identification Information:</u> • Username • Full Name	User access and authorization management.

	• Email Address • Password • IP Address(es) • MAC Address • Device ID • CPU Information • Time Zone • Uptime • Last Communication Time • Browser Information	
Generated Data	<u>Alert data ingested from connected sources may include generated data from integrated security products:</u> • Usernames / Account Identifiers referenced in alerts • Hostnames/Device IDs • Source/Destination IP Addresses • Email Addresses (e.g., phishing alert context) • File Names, Hashes, and Paths • Process Names and Command-Line Data • URLs/Domain Names • MAC Addresses <u>Wise's own investigation output:</u> • Usernames / Hostnames / (IOCs) • Investigation Reports and Summaries • Confidence Scores and Verdicts • MITRE ATT&CK technique mappings • Threat Evidence • Severity Ratings • Agent activity and reasoning/audit logs (timestamps, API calls to enrichment sources, human-in-the-loop actions)	Enterprise-wide threat analysis, compliance, and auditing, including to investigate and triage security alerts. To enrich alerts with context from connected sources. Also, to determine severity and generate verdicts, support threat hunting and remediation workflows.

	Analyst Feedback	
Collected Data	- Integration connection settings (API endpoints, filters) - Authentication credentials for connected systems - Alert-ingestion and enrichment configuration/policies - Investigation Context - Organizational Context	To configure and manage integrations with the Customer's connected security systems and enforce Customer-defined investigation and response policies. To enhance agent output. Also, to ground agent output in organizational context.

***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 Wise™ for Private Cloud data center locations vary depending on the data sharing license the Customer purchases from Trellix.

For virtual deployments with an offline license, the data center is located within the Customer's network infrastructure and no data is captured by Trellix Wise™ for Private Cloud.

Table 2a. Data Center Locations - offline license

Data Center Provider	Data Center Location
Not Applicable	Not Applicable

For virtual deployments with a one-way data sharing license, Trellix uses AWS and GCP to send contextual threat intelligence and content pack updates down to Customers from locations listed below, and no data is captured by Trellix Wise™ for Private Cloud.

For virtual deployments with a two-way data sharing license, Trellix uses AWS and GCP to send contextual threat intelligence and content pack updates down to Customers from locations listed below. Trellix Wise™ for Private Cloud also captures uploaded Customer telemetry data containing bug reports, threats and malware in locations listed below. Uploaded threat metadata is anonymized.

Table 2b. Data Center Locations - one-way and two-way data sharing licenses

Data Center Provider	Data Center Location
AWS	AWS West (Oregon)

AWS	AWS East (Virginia)
GCP	US West 1 (Oregon)
GCP	US West 2 (Los Angeles, California)
GCP	US West 3 (Salt Lake City, Utah)
GCP	US West 4 (Las Vegas, Nevada)
GCP	US Central 1 (Iowa)
GCP	US East 1 (South Carolina)
GCP	US East 5 (Columbus, Ohio)
GCP	US Central 2 (Oklahoma)
GCP	US East 4 (Northern Virginia)
GCP	US South 1 (Dallas, Texas)

Subprocessors

Trellix partners with service providers that act as subprocessors for the Trellix Wise™ for Private Cloud 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 3a. Subprocessors - offline license

Subprocessor	Personal Data Category	Service Type	Location of Data Center
Not Applicable	Not Applicable	Not Applicable	Not Applicable

Table 3b. Subprocessors - one-way and two-way license

Subprocessor	Personal Data Category	Service Type	Location of Data Center
AWS	Generated Data	Threat Intelligence sent to Customer	See Table 2b.
GCP	Generated Data	Threat Intelligence sent to Customer	See Table 2b.

Table 3c. Subprocessors - two-way license only

Subprocessor	Personal Data Category	Service Type	Location of Data Center
AWS	Generated Data	Threat Intelligence - uploaded anonymized threat metadata	See Table 2b.
GCP	Generated Data	Threat Intelligence - uploaded anonymized threat metadata	See Table 2b.
Pendo.io	Administrative Data	Analytics	Google Cloud Platform (United States: Iowa South Carolina Northern Virginia)

			Columbus Dallas Oregon Los Angeles Salt Lake City Las Vegas)
--	--	--	---

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 function. 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 Wise™ for Private Cloud to carry out the service, who can access that data, and why.

Table 4. Access Control

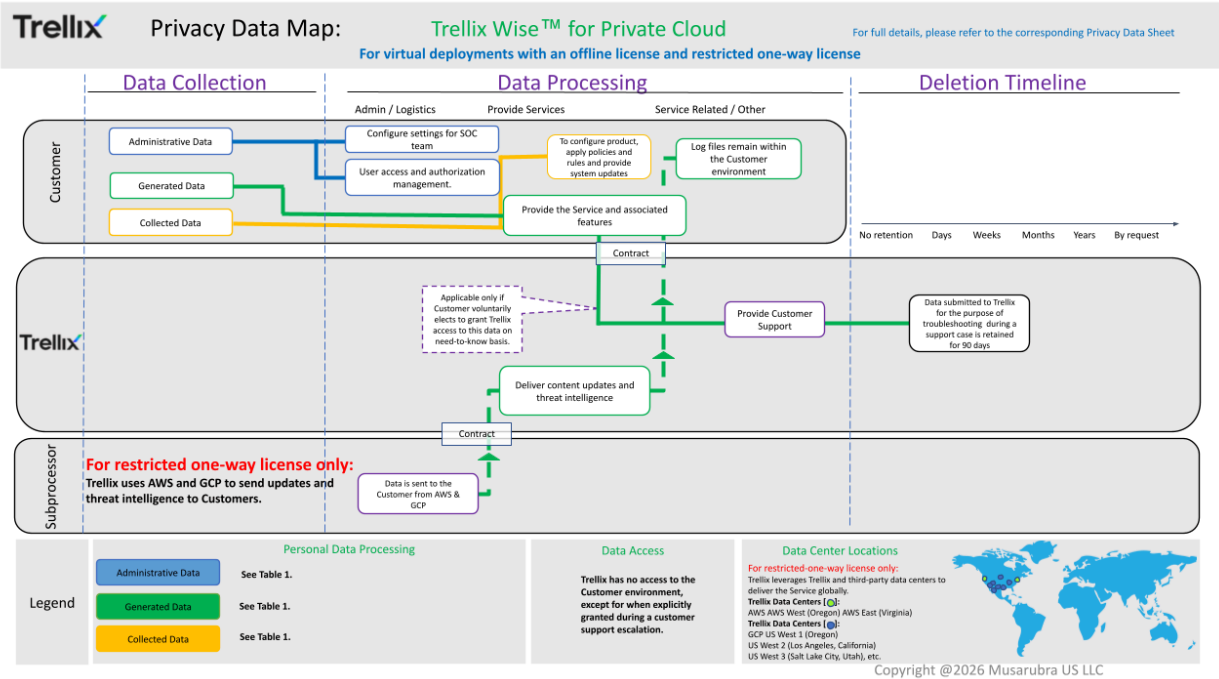
Personal Data Category	Who has access	Purpose of the access
Administrative Data	Customer: SecOps Admins.	Administration of access and roles. Identification and classification of assets monitored within the enterprise.

	Trellix: Customer support staff when granted access, or data is explicitly shared by the Customer.	For offline and one-way restricted licenses: No default access.
	Trellix two-way license: Trellix.	For two-way license: for improvement of services.
Generated Data	Customer: Users of the system granted access to analyze threats identified by the system.	To discern suspicious activities from normal activities.
	Trellix: Customer support staff when granted access, or data is explicitly shared by the Customer.	For offline and one-way restricted licenses: No default access. Analysis of escalated issue.
	Trellix two-way license: Trellix.	For two-way license: for product functionality and improvement of services.
Collected Data	Customer: System administrators, local IT support staff.	Monitoring of operations. Analysis of escalated issue.
	Trellix: Customer support staff when granted access, or data is explicitly shared by the Customer.	For offline and one-way restricted licenses: No default access. Analysis of escalated issue.
	Trellix two-way license: Trellix.	No default access.

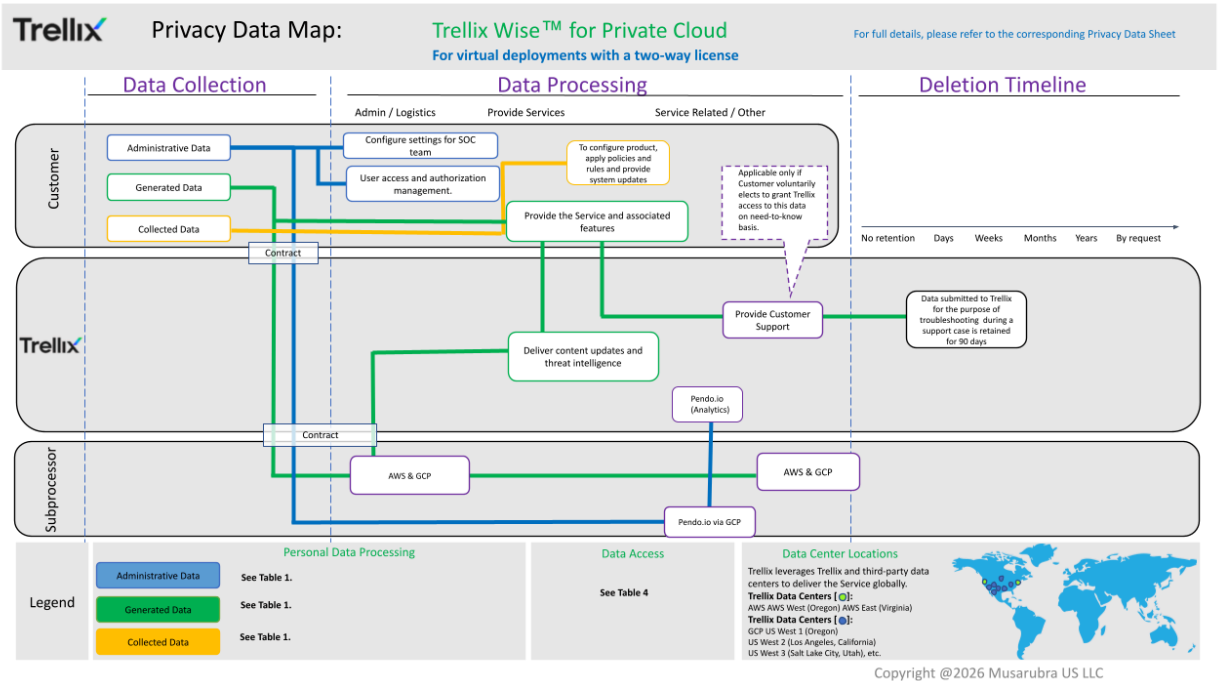
Trellix Wise™ for Private Cloud Data Flow Diagrams

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

Virtual deployment of Trellix Wise™ for Private Cloud (offline license and restricted one-way license):



Virtual deployment of Trellix Wise™ for Private Cloud (for connected two-way license):



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 Trellix Wise™ for Private Cloud service is enabled or disabled. When it is disabled, no data is processed, collected nor 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 Trellix Wise™ for Private Cloud 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 requests that all data be transferred to a third-party data store).

Data Deletion and Retention

The table below lists the personal data used by Trellix Wise™ for Private Cloud, 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 opening a case through the [Trellix Thrive portal](#). 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. Personal 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 using 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, or disclosure.

For a two-way license, Trellix Wise™ for Private Cloud sends data over SSL/HTTPS to Trellix's instance in AWS and GCP.

AWS and GCP audit and certify their environments on a regular basis by a third-party vendor. AWS and GCP are compliant with dozens of standards including NIST, ISO, SOC, CSA, PCI, GDPR, etc.

For AWS - The latest audit reports are available on the AWS website and can be found once logged into the AWS Console.

For additional details on AWS certifications, visit <https://aws.amazon.com/>

For GCP - The latest audit reports are available on the Google Cloud website and can be found once logged into Google's Compliance Reports Manager.

For additional details on GCP certifications, visit <https://cloud.google.com/compliance>.

Table 6. Personal Data Security

Personal Data Category	Type of Personal Data	Security Controls and Measures
Administrative Data	See Table 1	Encrypted in transit and 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 Wise™ for Private 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, Texas, 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, 2nd Floor, Suite 2200

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.

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.