Trellix **Privacy Data Sheet** We bring security to life.

Trellix Endpoint Detection and Response (EDR) with Trellix Wise

The purpose of this Privacy Data Sheet is to provide Customers of Trellix EDR 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 EDR 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 EDR subscription.

Trellix will process personal data from EDR 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 EDR to provide its functionality.

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

Product Overview

Trellix EDR is a SaaS service that enables Customers to detect, investigate, and respond to known and unknown cyber threats. The EDR service provides automatic, advanced, and continuous analytics of the Customer's enterprise endpoint system and detects suspicious activity across the entire enterprise.

Trellix's machine learning technologies provide guided investigations that automatically capture, summarize, and visualize evidence from sources that are identified as threats within the enterprise to dynamically analyze the detected threat as the investigation evolves. The EDR service provides an in-depth understanding of the detected threat and includes single-click response capabilities to enable Customers to respond to new and emerging threats quickly and confidently.

[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."

The EDR service captures information distributed across the Customer's entire endpoint system and integrates detection and response alert ranking so that Security Operators (SOs) quickly understand and respond to the impending threat.

Trellix EDR reduces the expertise and effort needed to perform a threat investigation and increases the speed with which SO's can determine the risk that a detected threat poses, and the root cause of the infected system. The EDR service continuously monitors Customer endpoints across the entire enterprise to detect suspicious behavior, then generates alerts mapped to the MITRE ATT&CK™ Framework. Trellix EDR then guides a Customer's Security Operations (Sec Ops) team through an investigation of the potential threat to contain actual threats and dismiss the alert.

A Customer's existing endpoint footprint and management system is enhanced with local and global threat intelligence to combat unknown and targeted malware instantly. Combined with other Trellix offerings (including, Trellix ePolicy Orchestrator (Trellix ePO)), the EDR service leverages the cloud to monitor and act on the full spectrum of new and emerging threats in real time, across all vectors—file, web, message, and network. The EDR service will initiate automatic actions against suspicious applications and processes and then quickly escalate responses against new and emerging forms of attack while informing other defenses and the global community.

Trellix EDR includes Trellix Wise Integration:

- **Enhances Trellix EDR capabilities —** Available as a feature in the **Monitoring, Device Search,** and **Historical Search** dashboards. Trellix Wise, a new Generative AI feature, provides the knowledge graph and the backing of real-time analysis to make data-driven decisions, optimize operations, and enhance the Customer experience. Trellix Wise enhances usability and helps you quickly analyze data generated from use of the service to significantly reduce the meantime to respond to threats. The Trellix Wise feature in the **Monitoring** dashboard and **Device Search** allows for two types of analysis methods, **Interactive mode** and **Dossier mode**, where the default analysis method is **Interactive mode**.

Trellix EDR with Trellix Wise is designed with two powerful tools:

- **Analysis:** The 'Ask Wise' button conducts a detailed analysis of any threat and provides recommended next steps.
- **Search:** Trellix Wise builds a search query using natural language questions in up to 50 different languages.

Trellix EDR includes the following security features:

- **Continuous real-time monitoring** — The **Monitoring** dashboard provides a visual representation of cyber threats detected on Customer enterprise endpoints running the EDR service.
- **Trellix Wise AI-Guided investigation** — Trellix Wise allows Customers to manage investigations of alerts and to analyze them using investigation guides.
- **Threat containment** — Customers can contain threats on the **Monitoring** dashboard; and during the investigation phase, Customers can stop and remove a threat, quarantine a device, dismiss a threat, or exclude a threat.
- **Real-time search** — Customers can use near real-time searches and historic search data based on collectors to obtain information from managed endpoints. This information can help further analyze a potential threat.
- **Historical search** — Historical search provides the type of information that is collected from the managed endpoints over a specified period. For historical search, queries are run in the cloud, while real-time search runs directly on endpoints to obtain the current data.
- **Collector's feature** — Customers use the collectors feature to capture process, file, network, system, and other built-in queries and store them in local databases at the endpoint. The captured data is retrieved and displayed within the EDR interface.
- **Threat hunting feature** — The threat hunting feature enables captured threat data to be manually stored at the endpoint. This data can then be retrieved from the endpoint and displayed on the Search pane within the EDR interface.
- **Tracing feature** — The tracing feature captures relevant trace data from Customer enterprise endpoints. The data is stored within the Customer's environment and is only evicted from the server if the size allocated to the server at the endpoint is reached at which point it is sent to Trellix's EDR instance in Amazon Web Services (AWS).
- **Snapshot feature** — The EDR service can take a snapshot of a device on-demand, capturing a comprehensive view of active processes, network connections, services, and autorun entries. Enabled by a non-persistence data collection tool, snapshots can be captured on both monitored and unmonitored systems.
- **Performance metrics** — Customers use the **Performance Metrics** dashboard to quickly get an overall status of all ongoing investigations. The trend graphs can help in assessing the allocation of resources and effort required in a Security Operations Center (SOC) to investigate and analyze potential threats.
- **Track action history** — Customers use the **Action History** page to view the details of all containment actions taken on a threat or device from the Monitoring and Investigating dashboards.

Trellix EDR can be implemented as one of two deployments:

- **Trellix EDR via ePolicy Orchestrator on Premise (ePO On - Prem)**: Customers use tenant credentials (Trellix Agent) for ePO On - Prem to create/deploy, manage, and enforce security policies. Customers can use the queries and dashboards options to track detections, activities, and status of their managed endpoint systems within their organization; or,

- **Trellix EDR via ePolicy Orchestrator SaaS (ePO - SaaS)**: Customers use tenant credentials (Trellix Agent) for ePO - SaaS to create/deploy, manage, and enforce security policies. Customers can use the queries and dashboards options to track detections, activities, and status of their managed Windows systems within their organization.

Please see Trellix Endpoint Detection and Response product sheet for additional information.

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

Personal Data Processing

The Trellix EDR service captures trace, process, and other threat event information, then correlates enterprise-wide endpoint data to provide a comprehensive view of all activity occurring across a Customer's distributed endpoints. The Trellix EDR service captures threat event information including the scripts executed, malicious files extracted, external connections established, and other relevant information necessary for the functionality of Trellix EDR. This captured event information becomes automatically available on the endpoint the instant a malicious event initiates.

When a Customer's ePolicy Orchestrator Administrator (ePO Admin) or Security Operator (SO) utilizes the Trellix EDR service, engagement information related to the operator who interacts with the EDR service is captured within EDR to grant access to the interface.

Captured engagement data is required to provide access to the comprehensive view of all endpoint activity occurring across the Customer's enterprise within a monitored network. Captured data enables the EDR service to detect and remediate malware proliferation within the enterprise. In addition, data captured from activities initiated by the SO is available in audit logs to ensure efficient performance of the service. Trellix will transfer information differently depending on the EDR deployment:

- **EDR Collected Data Transfer via ePO On-Prem:** The captured event information is sent via Trellix's EDR service to the Trellix Data Exchange Layer (DXL) by way of TLS version 1.2 encryption to Trellix Endpoint Detection and Response (EDR) server/database.
    - Note that data captured by the **Snapshot feature** is sent to ePO On-Prem by way of SSL/HTTPS connection to Trellix ePolicy Orchestrator (ePO On - Prem) server/database.
- **EDR Collected Data Transfer via ePO - SaaS:** The captured event information is sent automatically by way of Amazon Web Services (AWS) SDK end-to-end encryption to Trellix's instance in AWS regional clouds.

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

Table 1. Personal Data Processed by Trellix Endpoint Detection and Response

Personal Data Category*	Types of Personal Data Processed	Purpose of Processing

Administrative Data	ePO Administrator general identification information: ● Registered Owner ● Registry Key Details - Name, Value ● Username ● Email Address ● Phone Number ● Full Name Security Operator general identification information: ● Username(s) ● Password ● IP address ● Email address ● Mac address ● Tenant/Customer ID	Used to manage business operations ensuring compliance, provide reporting, and facilitate troubleshooting.
Generated Data	Incidents / Events: ● Windows Management Instrumentation Service Events ● Linux Audit Daemon generated events ● MacOS Security Framework events ● SourceURL ● EmbedFilename ● Path ● Trellix Agent GUID ● File Name ● Interactive Shell cmdline ● Source IP ● Destination IP Evidence: ● Telemetry Feedback ● Attributes reported by Trellix Endpoint protection ● Script Content ● Threat Event Logs ● Audit Logs ● Collectors Data	Endpoint management, compliance, auditing, and threat analysis.

Collected Data	Configuration information: ● Active directory Username ● System tag ● Product logs ● Trace Data	Used to Integrate with Customer management systems.

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 uses its own data centers as well as third-party infrastructure providers to deliver the service globally. EDR processes the personal data in Trellix's instance in Amazon Web Services, Inc. (AWS) regional clouds located in the United States, Australia, Canada, India, Germany, 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 2. Data Center Locations

Data Center Provider	Data Center Location
AWS	AWS East (Virginia)
AWS	AWS West (Oregon)
AWS	Australia (Sydney)
AWS	Canada (City)
AWS	India (Mumbai)
AWS	Europe (Frankfurt)

Subprocessors

Trellix partners with service providers that act as subprocessors for the EDR 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	See Table 1	Hosting	AWS East (Virginia)
AWS	See Table 1	Hosting	AWS West (Oregon)
AWS	See Table 1	Hosting	Australia (Sydney)
AWS	See Table 1	Hosting	Canada (City)
AWS	See Table 1	Hosting	India (Mumbai)
AWS	See Table 1	Hosting	Europe (Frankfurt)
AWS	See Table 1	Artificial Intelligence Services (Amazon Bedrock)	See Table 2

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 requests and performs 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 by 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.

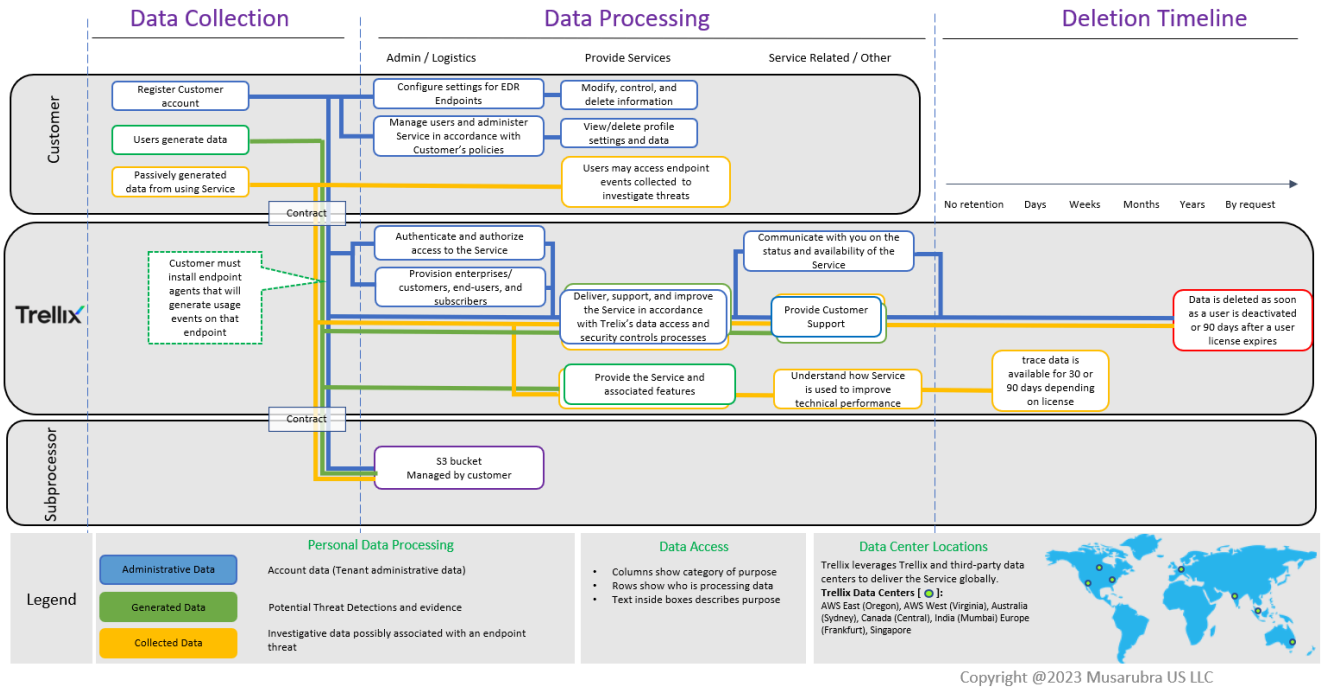
The table below lists the personal data used by the EDR service to carry out the service, who can access that data, and why.

Table 4. Access Control

Personal Data Category	Who has access	Purpose of the access
Administrative Data	Customer	Tenant Login, to associate data set with the Customer.
	Trellix	To administer and manage users.
Generated Data	Customer	To Investigate data associated with an endpoint threat.
	Trellix	To control data volumes and Investigate data errors.
Collected Data	Customer	To investigative data associated with an endpoint threat.
	Trellix	To control data volumes and Investigate data errors.

Trellix Extended Detection and Response (EDR) 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 EDR 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 the EDR service 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 EDR, 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	90 days following subscription expiry or immediately on customer request to delete account.	Compliance, reporting, troubleshooting.
Generated Data	30 days or 90 days depending on the SKU purchased.	Compliance, reporting.

Collected Data	30 days or 90 days depending on the SKU purchased.	System integrations.

Customer data transferred for investigations is retained for up to 12 months. Anonymized Customer data used in product improvement and threat research may be retained for an indefinite amount of time.

Customers can delete investigations created in Trellix Endpoint Detection & Response through the user interface. Deleted investigations will remove the investigation. Data deleted by the Customer may not be recoverable.

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.

Trellix EDR uses a secure portal hosted by AWS to store product data. Data collection is accomplished by downloading an executable tool to the Customer's environment where queries and API calls are performed against Trellix products. The collected data is then encrypted using 256-bit encryption as an output file and uploaded via secure SSL connection to the AWS Trellix server where it is processed and stored in the encrypted database.

AWS audits and certifies their environment on a regular basis by a third-party vendor. AWS is compliant with dozens of standards including NIST, ISO, SOC, CSA, PCI, GDPR, etc. 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/.

- Search for "Artifact"
- Select Artifact from the search results
- Select View Reports from the AWS Artifact page

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 EDR 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 (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, 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.