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

Trellix Managed Detection and Response (MDR)

The purpose of this Privacy Data Sheet is to provide Customers of Trellix - MDR 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 telemetry capabilities on their overall privacy posture.

Trellix MDR 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 MDR subscription.

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

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

Product Overview

The Trellix MDR security platform is an advanced 24/7 security control that includes a range of fundamental security activities, including cloud-managed security, specifically for organizations that cannot maintain their own security operations center. Trellix's MDR service combines advanced analytics, precise threat intelligence, and human expertise in incident investigation, response, and remediation, which is deployed at the host and network levels.

By combining artificial intelligence (AI) and machine learning (ML)-led advanced threat intelligence, 24/7 monitoring, and expert response capabilities, Trellix MDR helps businesses detect and mitigate cyber threats with increased precision and speed. Trellix MDR delivers continuous threat monitoring, incident response, and remediation of threats and integrates with other Trellix Endpoint Security Solutions, including Endpoint Security (ENS) and Endpoint Forensics (HX), Endpoint Detection and Response (EDR),

[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."

ePolicy Orchestrator (ePO), Insights (IN) and Wise to provide end-to end threat monitoring, incident response, and remediation of Customer security operations.

The MDR service provides an alternative to the constant chase for the latest technology in advanced security products by integrating Endpoint Detection and Response (EDR) solutions that can become a challenge for security operations teams to learn and maintain.

As a result, a Customer's level of threat monitoring, detection, and analysis are improved without the challenge and expense required to keep an internal security team fully staffed and up to date with the latest threat information.

Trellix MDR's AI-powered precision increases detection speed, response time and drives adept, automatic and continuous analysis and security posture improvements to harden your defenses.

Trellix MDR services are not just limited to greater detection and response capabilities. The MDR service provides constant updates to prevent, detect, and defend against evolving attacks by generating a continuous feedback loop from Trellix Endpoint Detection and Response (EDR) to Customer endpoint protection policies and the Customer's network environment. The MDR service also provides proactive intelligence and defense insights into advanced threats that overwhelm security teams. Detection levels are improved while breach dwell times are reduced.

Trellix MDR includes the following security features:

- Complete managed endpoint threat detection and response service including:
    - 24/7 monitoring, analysis, detection, and response with experienced Security Operations Center (SOC) analysts
- Blind spot detection and tuning of Customer Trellix ePO environments
- Continuous optimization of Customer Trellix EDR and Endpoint Security deployments
- On-demand expertise from an elite team of Trellix security experts
- Improved forensics and higher-level investigations
- Vulnerability management
- Major incident response and log management

Trellix MDR 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 Customers quickly analyze data generated from use of the service to significantly reduce mean time 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 MDR can be implemented as one of two deployments:

- **Trellix MDR 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 systems within their organization; or,

- **Trellix MDR 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 systems within their organization.

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

Please also see Trellix Endpoint Detection and Response (EDR), 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 MDR service captures trace, process, and other threat event information then correlates Customer-wide endpoint data to provide a comprehensive view of all activity occurring across a Customer's distributed endpoints.

Trellix's MDR analysts have a deep understanding of your Trellix ENS, Trellix EDR, Trellix ePO, Trellix IN and Trellix Wise tools to rapidly implement, configure, optimize, and begin monitoring your environment. When a potential threat is detected, it is immediately escalated to Trellix MDR's expert SOC analysts, who conduct an in-depth investigation. Trellix's MDR analysts determine the nature of the threat, respond to the threat, and make any changes necessary to Customer configuration, rules, alerts, or policies to strengthen Customer defenses against the same or similar threats in the future.

The Trellix MDR service captures alert data from other Trellix Endpoint Security Solutions where the captured data may include personal data such as IP & MAC addresses, filenames & locations, timestamps, hostnames, device name, user name, alert data, system configuration state, system event codes and geolocation information.

Customers may input personal data into key fields used by MDR depending on Customer configuration. Moreover, when a Customer's ePolicy Orchestrator Administrator (ePO Admin) or Security Operator (SO) utilizes the Trellix MDR service, administrative data related to the SO who interacts with the MDR service is captured within MDR to grant access to the interface.

Captured administrative 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 MDR 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. Therefore, Trellix may transfer information differently depending on the MDR deployment:

- **MDR captured data transfer via ePO On-Prem**: The captured information is sent via Trellix's MDR 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.

- **MDR captured data transfer via ePO - SaaS**: The captured 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, Trellix MDR may process a range of data potentially containing personal information. The table below shows the personal data processed by Trellix MDR to provide its services and describes why the data is processed.

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

Personal Data Category*	Types of Personal Data Processed	Purpose of Processing
Administrative Data	ePO Administrator General Identification Information: ● Email Address ● Phone Number ● Full Name Security Operator General Identification Information: ● Tenant/Customer ID	Incident investigation escalation.
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	Incident investigation escalation.

	• Collectors Data	
Collected Data	Configuration information: • Active Directory Username • System Tag • Product Logs • Trace Data	Incident investigation escalation.

***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 Trellix ePO - On Prem deployment, the data center is located within the Customer's network infrastructure.

For Trellix ePO - SaaS deployment, Trellix uses its own data centers as well as third-party infrastructure providers to deliver the service globally. Trellix MDR may process the personal data in Trellix's instance in Amazon Web Services, Inc. (AWS) regional clouds located in the United States, Germany, Australia, Japan, Singapore, and India. 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	Germany (Frankfurt)
AWS	Australia (Sydney)
AWS	Canada (Montreal)
AWS	India (Mumbai)

Subprocessors

Trellix partners with service providers that act as subprocessors for the Trellix MDR 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
Reveald	See Table 1	Managed Detection and Response	See Table 2.
AWS	See Table 1	Hosting	See Table 2.
AWS	See Table 1	Hosting	See Table 2.
AWS	See Table 1	Hosting	See Table 2.
AWS	See Table 1	Hosting	See Table 2.
AWS	See Table 1	Hosting	See Table 2.
AWS	See Table 1	Hosting	See Table 2.
AWS	See Table 1	Hosting	See Table 2.
AWS	See Table 1	Hosting	See Table 2.
Okta	See Table 1	Authentication	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 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.

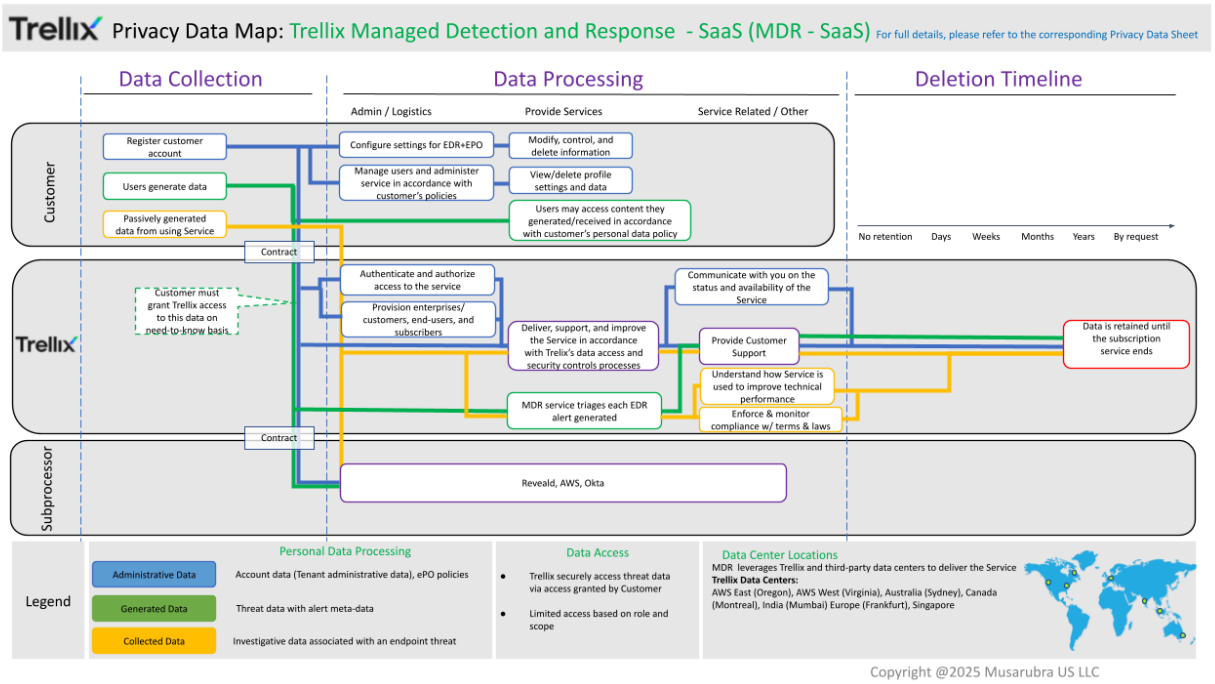
The table below lists the personal data used by Trellix MDR to carry out the service, who can access that data, and why.

Table 4. Access Control

Personal Data Category	Who has access	Purpose of the access
Administrative Data	Customer	Alert inspection, investigation and incident response, reporting.
	Trellix	Alert inspection, investigation and incident response, reporting.
Generated Data (Incidents / Events)	Customer	Alert inspection, investigation and incident response, reporting.
	Trellix	Alert inspection, investigation and incident response, reporting.
Generated Data (Evidence)	Customer	Alert inspection, investigation and incident response, reporting.
	Trellix	Alert inspection, investigation and incident response, reporting.
Collected Data	Customer	Alert inspection, investigation and incident response, reporting.
	Trellix	Alert inspection, investigation and incident response, reporting.

Trellix MDR 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 Trellix MDR 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 Trellix MDR 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 Trellix MDR, 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 sending an email request 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	Retained until the subscription service ends.	Customer Service.
Generated Data	Retained until the subscription service ends.	Customer Service and Troubleshooting.
Collected Data	Retained until the subscription service ends.	System integrations.

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 MDR 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 Trellix MDR 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, 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.