Trellix Privacy Data Sheet We bring security to life.

Trellix Endpoint Detection and Response with Forensics - On-Premise (EDRF - On-Prem)

The purpose of this Privacy Data Sheet is to provide Customers of Trellix EDRF - 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 EDRF - On-Prem is a solution that protects servers, computer systems, laptops, and tablets against known and unknown threats like malware, suspicious communications, unsafe websites and files, which is provided to companies or persons who obtain a Trellix EDRF - On-Prem subscription.

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

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

Product Overview

Trellix EDRF - On-Prem helps organizations identify, contain, and remediate security threats, minimizing potential damage to the organization. Trellix's EDRF - On-Prem is an on-premise endpoint security solution that monitors and analyzes endpoint activity within the organization's network infrastructure. It collects telemetry on processes, file and registry changes, network connections, and user activity.

[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."

Trellix EDRF - On-Prem extends and enhances current EDR capabilities to provide new, granular and more sophisticated levels of visibility needed to detect, investigate, and respond to deeply rooted and obfuscated threats, as well as the dreaded “patient zero” malware. Trellix EDRF - On-Prem combines Trellix Endpoint Detection and Response’s (EDR) real-time threat detection with Trellix Endpoint Security’s (HX) forensics investigative capabilities.

Trellix EDRF - On-Prem is integrated with Trellix Forensics which helps security analysts accurately surface suspicious behavior, make sense of alerts, collect forensic data, and take informed action. EDRF - On-Prem continues to capture data both in online and offline modes and, enabled by a nonpersistent data collection tool, also captures snapshots on both monitored and unmonitored systems.

Trellix EDRF - On-Prem supports continuous endpoint visibility and post-incident investigation without reliance on cloud services. Security teams use locally stored telemetry to detect suspicious behavior, conduct historical analysis, and perform compliance-driven reviews across the Customer’s network infrastructure.

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

- **Comprehensive Detections** — Accelerates malware protection through machine-learning, behavior analysis, indicators of compromise (IOCs), custom IOCs and unparalleled visibility.
- **Integrated Workflows** — Integrates Trellix EDR, Forensics, and ePO workflows to detect, investigate, analyze and remediate threats.
- **Enterprise Search** — Enables easy discovery and investigation of suspicious activity.
- **Rapid-Data Acquisition** — Uses the rapid data acquisition feature to conduct in-depth endpoint analysis over a specific timeframe.
- **Continuous Real-Time Monitoring** — Provides a visual representation of cyber threats detected on Customer enterprise endpoints running the EDRF - On-Prem service via the Monitoring dashboard.
- **MITRE ATT&CK™ Mapping** — Maps behavior based detection results to the MITRE ATT&CK™ framework, supporting a consistent process to prioritize responses by determining the phase of a threat and its associated risk.
- **Forensics Functionality** — Supports security investigations through targeted, customizable forensic data collection. Investigators can capture comprehensive endpoint snapshots—including active processes, memory configurations, network connections, registry keys, and partial or full disk images—by selecting specific attributes across 11 event types.
- **Historical Search Capabilities** — Empowers security teams to investigate historical incidents and events to proactively hunt for threats. The historical search feature enables threat detection by querying a centralized virtual appliance, the EDR Telemetry Store, for incident and event data from all endpoint devices.

Trellix EDRF - On-Prem can be implemented as one of two deployments:

- **Standalone deployment of Trellix HX** - Deployment occurs via a custom appliance purchased from Trellix and installed within the Customer's enterprise environment.

- **Virtual deployment of Trellix HX**- Customers manage the deployment via their hosted ESXi / Nutanix / Hyper-V or private Azure / AWS cloud.

***Trellix EDRF On-Prem is configured via Trellix ePolicy Orchestrator On-Premise (ePO On - Prem)**: Customers use ePO On-Prem to create/deploy, manage, and enforce security policies and use the queries and dashboard options to track detections, activities, and the status of their endpoint systems within their organization.

Please see Trellix Endpoint Detection and Response with Forensics (EDRF) product sheet for additional information.

Please also see, Trellix ePolicy Orchestrator on Premise (ePO On-Prem) and Trellix Endpoint Security (HX) Privacy Data Sheets for additional information.

Personal Data Processing

Trellix EDRF - On-Prem operates by capturing data from Customer endpoints and sending it to a central management platform for analysis and action. To provide the service, Trellix EDRF - On-Prem logs relevant activities on Customer endpoints to capture a comprehensive view of active processes, network connections, services, registry keys, and autorun entries that support Security Operations investigations.

The Trellix EDRF - On-Prem service captures trace, process, file, 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 EDRF - On-Prem service also captures the executed scripts and files, established external connections, and other relevant information.

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

Captured engagement and event data enables the EDRF - On-Prem service to detect and remediate attacks 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.

Moreover, EDRF - On-Prem provides forensics capabilities to provide enhanced investigation and containment capabilities. Integrated forensic data collection allows security teams to capture and store files, memory, and processes, as well as partial and full disk images, for further analysis and investigation. EDRF - On-Prem sends out the alerts, data triages, and search results to the HX server, where, based on the server configurations, the threats can be detected, enriched, and contained.

Trellix EDRF includes optional integration with Trellix Dynamic Threat Intelligence (DTI) cloud, which provides Customers with the latest intelligence on advanced cyber attacks. Trellix DTI cloud is also used to enable automatic software updates. Trellix EDR-F enables Customers to access Trellix DTI cloud depending on Customer license, including one-way, two-way, and offline licenses.

With a one-way sharing license, Customers can access Trellix DTI to receive the latest intelligence from Trellix, where no telemetry data is shared back to Trellix from the Customer environment.

With a two-way sharing license, Trellix EDRF Customers automatically receive the latest threat intelligence from Trellix DTI. This also enables Customers to share telemetry about threats and malware identified in the Customer environment back with Trellix to improve the overall detection efficacy of the EDRF.

With an offline license, Customers do not access Trellix DTI cloud and no data is submitted to or from Trellix DTI cloud, where data processed by Trellix EDRF - On-Prem remains within the Customer's local infrastructure, supporting environments with strict data residency, regulatory, or air-gapped requirements.

- **Standalone deployment of HX:** The solution reads data stored within the Customer's network environment and no data is captured by Trellix.
- **Virtual deployment of HX:** The solution reads data stored within the Customer's network environment and no data is captured by Trellix.

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

Table 1. Personal Data Processed by Trellix Endpoint Detection and Response with Forensics - On-Premise

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 ● First Name ● Last Name Security Operator General Identification Information: ● Username(s) ● Password	Used to manage business operations ensuring compliance, provide reporting, and facilitate troubleshooting.

	● IP Address ● Email Address ● Mac Address ● Device Serial Number ● CPU Information ● Tenant/Customer ID ● Browser Information	
Generated Data	<u>Incidents / Events</u>: ● File Data Written ● Network Destinations ● DNS Lookups ● Registry Data ● Application Data ● Name Pipes ● API Events ● Activity Timestamps ● Network Address Updates ● eBPF Sensor <u>Evidence</u>: ● Recent Process Activity on Device ● Browser History ● Data on Disk ● Data within Active Memory ● Command Line History ● Registry Data ● DNS Lookups ● Network Activity ● Image Load Event (DLL)	Used to discern suspicious activities from normal activities. Endpoint management, compliance, auditing, and threat analysis.
Collected Data	<u>Configuration Information</u>: ● Active Directory Username ● System Tag ● File ● Trace/Event History ● Product / Audit Logs	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 EDRF - On-Prem data center locations vary depending on the data sharing license the Customer purchases from Trellix.

For standalone and virtual deployments with an offline license, the data center is located within the Customer's network environment.

Table 2a. Data Center Locations

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

For standalone and virtual deployments with one-way or two-way data sharing license.

Trellix uses its own data centers as well as third-party infrastructure providers to deliver the service globally. Trellix Dynamic Threat Intelligence (DTI) - cloud processes the personal data in Trellix's instance in Amazon Web Services, Inc. (AWS) regional clouds located in the United States.

Table 2b. Data Center Locations

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

Subprocessors

Trellix partners with service providers that act as subprocessors for the EDRF - 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 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 or two-way sharing license)

Subprocessor	Personal Data Category	Service Type	Location of Data Center
AWS	See Table 1.	Hosting	See Table 2b.

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 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.

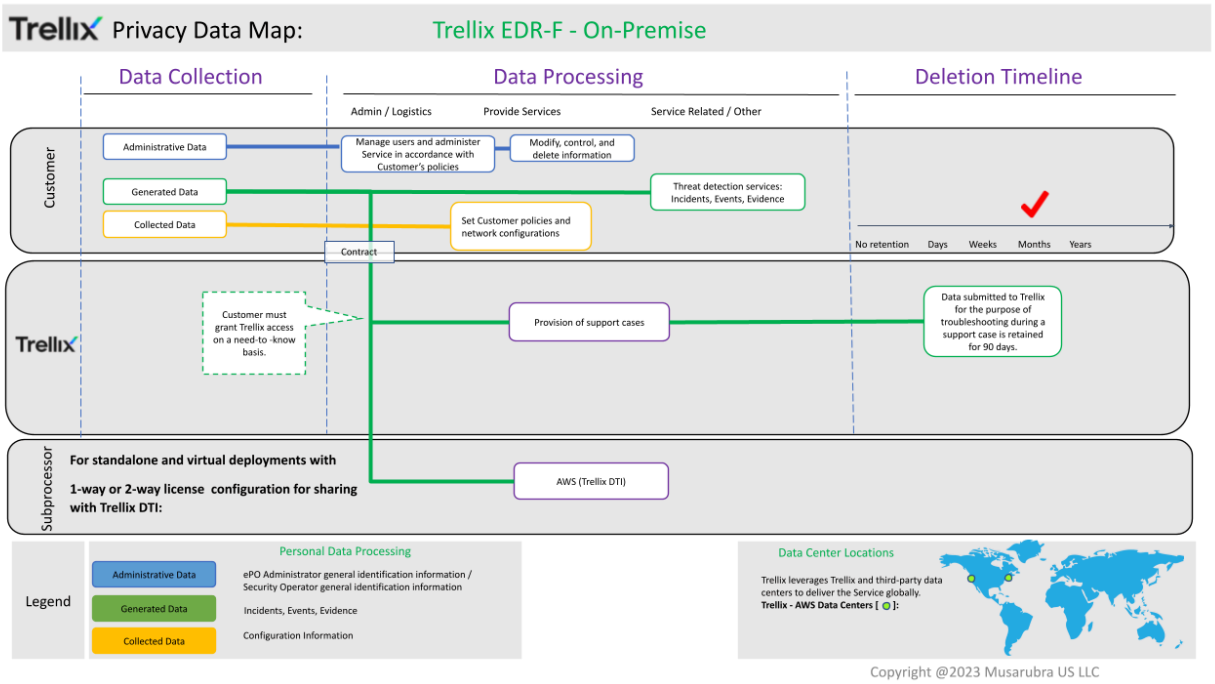
The table below lists the personal data used by the EDRF - On-Prem service to carry out the service, who can access that data, and why.

Table 4. Access Control

Personal Data Category	Who has access	Purpose of the access
Administrative Data	Customer	Access and role administration. Identification and classification of endpoints monitored within the enterprise.
	Trellix	Analysis of escalated issue.
Generated Data	Customer	Analysis of escalated issue.
	Trellix	No Access.
Collected Data	Customer	Monitoring of operations.
	Trellix	Analysis of escalated issue.

Trellix Endpoint Detection and Response (EDRF - On-Prem) 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, 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.

Data Portability

Except with respect to Registration Information, the Customer can forward the personal data processed by the EDRF - On-Prem 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 EDRF - 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 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. 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 implements rigorous technical and organizational security controls designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

For standalone and virtual deployments with one-way or two-way sharing license.

Trellix DTI 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.

Generated Data	See Table 1	Encrypted in transit.
Collected Data	See Table 1	Encrypted in transit.

*Additional details for product certifications are available upon request.

Compliance with Privacy Requirements

Trellix is committed to protecting personal data. 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.