Trellix Privacy Data Sheet We bring security to life.

# Trellix Endpoint Security (ENS) - Linux

The purpose of this Privacy Data Sheet is to provide Customers of Trellix ENS - Linux 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 ENS - Linux is a solution which protects servers, computer systems, laptops and tablets against known and unknown threats like malware, suspicious communications, unsafe websites and files, and is made available by Trellix to companies or persons who obtain a Trellix ENS – Linux subscription.

Trellix will process personal data from ENS - Linux 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 the ENS - Linux service to provide its functionality.

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

## Product Overview

Trellix ENS – Linux is an integrated, extensible security solution that protects servers, computer systems, and laptops against known and unknown threats. ENS - Linux enables Customers to respond to and manage the threat defense lifecycle with proactive defenses and remediation tools. Automatic rollback remediation returns systems to a healthy state to keep users and administrators productive. This saves time that users might otherwise spend waiting for system remediation, performing recovery, or reimaging an infected machine.

Combined with other Trellix SaaS offerings (including, for example, Trellix Global Threat Intelligence (Trellix GTI)), the Trellix Endpoint Security framework 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.

[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 existing endpoint footprint and management system is enhanced with localized and global threat intelligence to combat unknown and targeted malware instantly. Automatic actions against suspicious applications and processes quickly escalate responses against new and emerging forms of attack while informing other defenses and the global community.

**ENS - Linux consists of the following security modules:**

- **Threat Prevention (TP)** (malware detection); Prevents threats from accessing systems, scans files automatically when they are accessed, and runs targeted scans for malware on client systems.
- **Adaptive Threat Protection (ATP)** (based on reputation and rules); Analyzes content from the Customer's enterprise and decides how to respond based on file reputation, rules, and reputation thresholds. Adaptive Threat Protection is an optional Trellix ENS - Linux module.

All modules integrate into a single Trellix ENS - Linux interface on the client system. Each module works together and independently to provide several layers of security.

**ENS - Linux can be deployed as one of two versions:**

- **Standalone deployment of ENS - Linux** — Available to install by the Customer's systems administrator to configure settings through the interface;
- **Managed deployment of ENS – Linux** — Available as one of two configuration options:

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

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

Please see Trellix Endpoint Security product sheet for additional information.

Please also see Trellix 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 ENS – Linux solution uses Trellix machine learning technology to proactively and automatically monitor and detect malicious activity and policy violations occurring on the Customer's enterprise endpoints. The ENS – Linux solution provides analysis of detected threat activity and policy violations. Trellix's machine learning modules analyze event information, in online and offline modes, from the Customer's enterprise endpoints and decide how to respond based on file reputation, rules, and

reputation thresholds, for both traditional and advanced file-less threats. Trellix will capture information differently depending on the ENS – Windows deployment version:

- **Standalone deployment of ENS – Linux;** The ENS - Linux solution reads data stored on the Customer's enterprise endpoints and no data is ever captured by Trellix.
- **Trellix ePolicy Orchestrator on Premise (ePO On - Prem) deployment;** The captured event information is sent automatically to Trellix Agent by way of SSL/HTTPS connection to Trellix ePolicy Orchestrator (ePO On - Prem) server/database present on the Customer's premises.
- **Trellix ePolicy Orchestrator SaaS (ePO - SaaS) deployment;** The captured event information is sent automatically to Trellix Agent by way of SSL/HTTPS connection to Trellix's instance in Amazon Web Services (AWS) regional clouds.

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

**Table 1. Personal Data Processed by Trellix Endpoint Security - Linux**

| Personal Data Category* | Types of Personal Data Processed | Purpose of Processing |
|---|---|---|
| Administrative Data | General identification information:<br>● IP address<br>● TA Agent (UID - randomly generated)<br>● Connection ID (ccuid)<br>● Device name<br>● Mac address<br>● System tag<br>● Username | Used to manage business operations ensuring compliance, provide reporting, and facilitate troubleshooting. |
| Generated Data | Incidents/Events:<br>● Threat details<br>○ Threat Name<br>○ Location<br>○ Action taken<br><br>Evidence:<br>● File Name<br>● File Path | Endpoint management, compliance, auditing, and threat analysis. |
| Collected Data | Configuration information:<br>● Product logs | Used to Integrate with user management systems. |

***The Personal Data Categories used in this, and other Trellix Privacy Data Sheets are:**

- **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 versions,** all data is stored on the Customer's enterprise endpoints and no data centers are utilized by the service.

**For Trellix managed ENS – Linux deployment,** Trellix uses its own data centers as well as third-party infrastructure providers to deliver the service globally. ENS – Linux processes the personal data in Trellix's instance in Amazon Web Services, Inc. (AWS) regional clouds located in the United States, Germany, Australia Singapore, and India. Trellix's regional clouds provide options to address Customers' data location preferences. 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 West (Oregon) |
| **AWS** | Germany (Frankfurt) |
| **AWS** | Australia (Sydney) |
| **AWS** | Singapore |
| **AWS** | India (Mumbai) |

## Subprocessors

**For Trellix managed ENS – Linux deployment,** Trellix partners with service providers that act as subprocessors for the ENS - Linux 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 West (Oregon) |
| **AWS** | See Table 1 | Hosting | Germany (Frankfurt) |
| **AWS** | See Table 1 | Hosting | Australia (Sydney) |
| **AWS** | See Table 1 | Hosting | Singapore |
| **AWS** | See Table 1 | Hosting | India (Mumbai) |

## 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 ENS - Linux to carry out the service, who can access that data, and why.

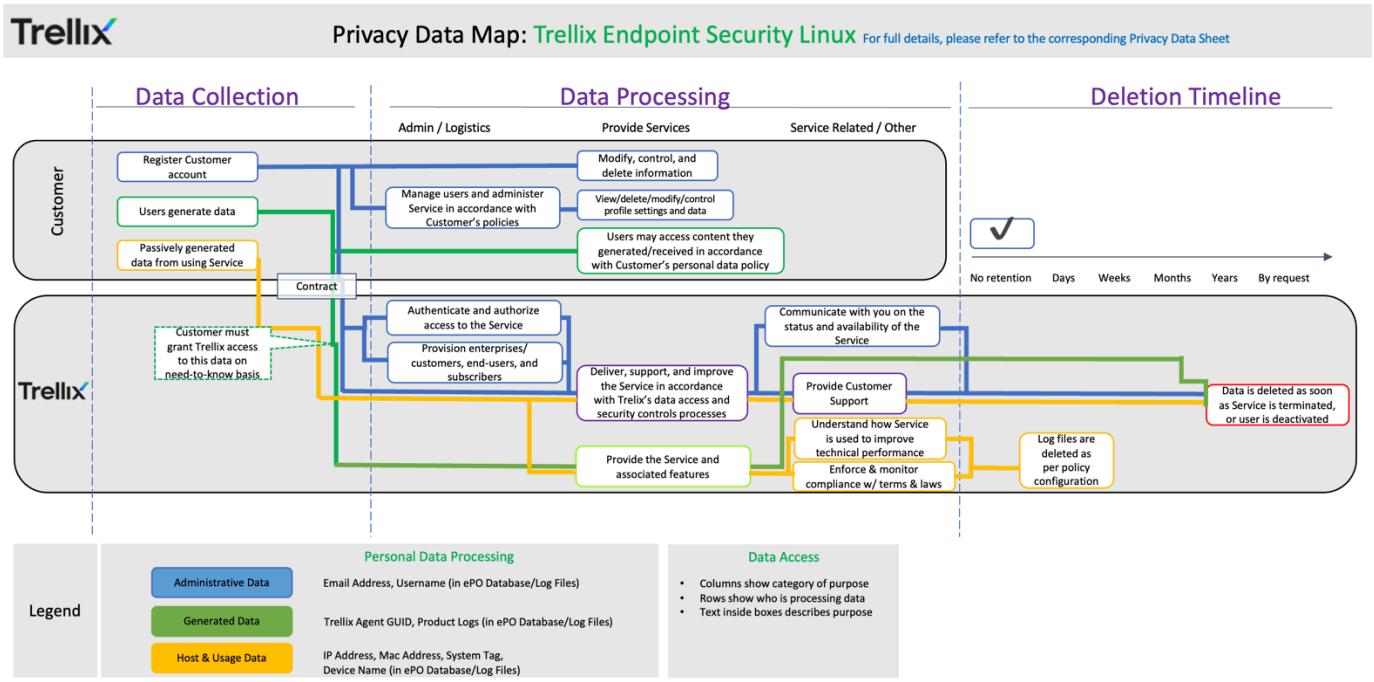
**Table 4. Access Control**

| Personal Data Category | Who has access | Purpose of the access |
|---|---|---|
| Administrative Data | Customer | Analysis of User/Systems suspected of malware detection/detonation and cleanup or quarantine of the same. Also, to provide data on suspected violations of policy, compliance, and reporting. |
| | Trellix | Debugging of Customer/operational data in the event of an escalation. |
| Generated Data (Incidents / Events) | Customer | Analysis of User/Systems involved in violations, compliance, and reporting. |

| | | |
|---|---|---|
| | Trellix | Debugging of Customer/operational data in the event of an escalation. |
| Generated Data (Evidence) | Customer | Associate evidence to a violation reported by ENS – Linux. |
| | Trellix | No access. |
| Collected Data | Customer | Manage user/machine/group policies and configurations and fine tune the systems as needed. Also, to associate evidence with a reported violation by ENS – Linux. |
| | Trellix | To give functionality to apply policies based on configuration. |

## Trellix Endpoint Security ENS - Linux 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 ENS - Linux 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 has the ability to forward personal data processed by ENS - Linux 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., if the 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 ENS - Linux, 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 contacting us 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 Customer removes associated endpoint | Compliance, reporting, troubleshooting. |
| Generated Data | 90 days or 365 days depending on the SKU purchased | Compliance, reporting. |
| Collected Data | Retained until the Customer deletes | 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.

**For Trellix managed deployments of the ENS – Linux service:**

ENS – Linux uses a secure portal hosted by AWS to store engagement 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 certification are available upon request.

## Compliance with Privacy Requirements

Trellix is committed to protecting personal data processed in global and regional product 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 Trellix 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. Trellix ENS – Linux 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 may 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.

Where Trellix is a Data Processor, users may be redirected to the Data Controller (e.g., the user's employer) or other organization for an appropriate 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 Data Sheet

Trellix Privacy Data Sheets are reviewed and updated on an annual, or as needed, basis.

The information provided with this document is for general awareness only, may be subject to change, and does not constitute legal or professional advice. Except as provided by the terms of a written agreement, the information and services described herein are provided "as is" with no warranty of any kind.