Trellix Privacy Data Sheet We bring security to life.

Trellix Enterprise Security Manager (ESM)

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

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

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

Product Overview

Trellix ESM is a foundational Trellix Security Incident Event Management (SIEM) solution that delivers performance, actionable intelligence, and solution integration at the speed and scale required for Trellix Customers' security organization. It allows the enterprise to quickly prioritize, investigate, and respond to hidden threats and meet compliance requirements.

ESM delivers real-time visibility to all activity on Trellix Customers' systems, networks, database, and applications. ESM also provides a deep understanding of the cyber environment outside of the Customer's enterprise endpoints, including cyber threat information and reputation feeds—as well as a view of the systems, data, risks, and activities inside the Customer's enterprise. It offers the Customer's

[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."

security team complete and correlated access to the content and context needed for fast, risk-based decisions, so a Customer can optimize its security posture in a dynamic threat and operational landscape.

ENS makes cyber threat and compliance management a core part of security operations, and also provides integrated tools for configuration and change management, case management, and centralized policy management. Additionally, content packs offer prebuilt configurations for advanced security use cases that help simplify security operations.

Combined with other Trellix SaaS offerings (including, for example, Trellix Global Threat Intelligence (Trellix GTI), Trellix ePolicy Orchestrator On-Premises (Trellix ePO – On-Prem), Trellix Intelligent Sandbox, and Trellix Threat Intelligence Exchange (Trellix TIE)), the Trellix Enterprise Security Manager 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.

Evolving security challenges require open, collaborative approaches to detect cyber-threats, reduce risk, and ensure compliance. Trellix ESM integrates with other Trellix products to resolve threats quickly without overloading resources.

Trellix ESM includes the following security features:

- Analyst-centric dashboards, reports, reviews, rules, and alerts;
- Content packs - prepackaged sets of alarms, views, reports, variables, correlation rules, and watchlists that address common security use cases;
- Predefined dashboards, audit trails, and reports for global regulations and control frameworks;
- Customizable compliance reports, rules, and dashboards;
- Ability to enrich events with contextual information (such as privacy solutions; threat data and reputation feeds; and identity and access management systems);
- Near real-time or historical aggregation and correlation of suspicious or confirmed threat information against event data;
- Ability to collect data from third-party security vendor devices and threat intelligence feeds;
- On-demand queries, forensics, rules validation, and compliance; and
- SOAR support, executing SOAR playbooks.

Trellix ESM can be implemented as one of two deployments:

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

- **Virtual deployment of ESM -** Customers manage the deployment of Trellix ESM on their hosted VMware ESXi, Linux KVM, Hyper-V or private Azure, AWS clouds, or Oracle Cloud Infrastructure (OCI).

Please see Enterprise Security Manager for additional information related to the Trellix Endpoint Security solution.

Personal Data Processing

ESM captures, processes, and analyzes information from various sources. The Trellix ESM solution captures third-party event data from network devices, applications, and endpoints. Captured information includes logs and events generated by network devices, such as firewalls, routers, and switches, as well as data from servers, applications, and endpoints. ESM also integrates with other security tools, such as intrusion detection and prevention systems, antivirus solutions, and vulnerability scanners, to gather additional information about potential threats.

The Customer determines whether to interconnect and configure devices or data sources located in different locations to send the captured information to the ESM solution. Note that Trellix does not have access to the captured data unless it is provided by the Customer for Customer support cases. Once the information is captured, ESM processes and normalizes the information to create a unified view of the security landscape.

For Standalone and Virtual deployments of ESM - The ESM solution captures data stored within the Customer's own network infrastructure.

For overflow data, note that by default, older data partitions are automatically deleted unless the Customer integrates an archival storage location.

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

Table 1. Personal Data Processed by Trellix Enterprise Security Manager

Personal Data Category	Types of Personal Data Processed	Purpose of Processing
Administration Data	General identification information: ● Username ● User IDs ● Sender Email Address ● Recipient Email Address ● Source IP Address ● Destination IP Address ● Device IDs ● MAC Addresses ● IP Geolocation ● Protocol Information ● Port Numbers ● IP Addresses ● Geolocation Data ● Email Addresses	Authentication and access control. Network traffic analysis and monitoring. Device identification and tracking. Email security analysis.
Generated Data	Incidents / Events: ● Endpoint Event Logs ● User Activity Logs	Security event correlation and analysis. File activity monitoring and threat detection. Location-based threat analysis.

	Evidence: • File Metadata • Threat Intelligence • Vulnerability Data • File Names • File Sizes	Network behavior analysis and intrusion detection. Network traffic analysis and monitoring. Device identification and tracking. Email security analysis.
Collected Data	Configuration information: • Application Logs • Application Data • API Logs • Software Versions • Patch Levels • Log Data • Audit Logs • Indicators of Compromise (IOCs) • System Logs • Network Traffic Data	Application performance and security monitoring. Vulnerability assessment and management. proactive threat detection and prevention. Compliance monitoring and auditing. Network traffic analysis and monitoring. Device identification and tracking. Email security analysis.

*** 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 standalone or virtual deployments, the data center is located within the Customer's own network infrastructure.

Table 2. Data Center Locations

Data Center Provider	Data Center Location
Not Applicable	Not Applicable

Subprocessors

Trellix partners with service providers that act as subprocessors for the ESM 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
Not Applicable	Not Applicable	Not Applicable	Not Applicable

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 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 ESM to carry out the service, who can access that data, and why.

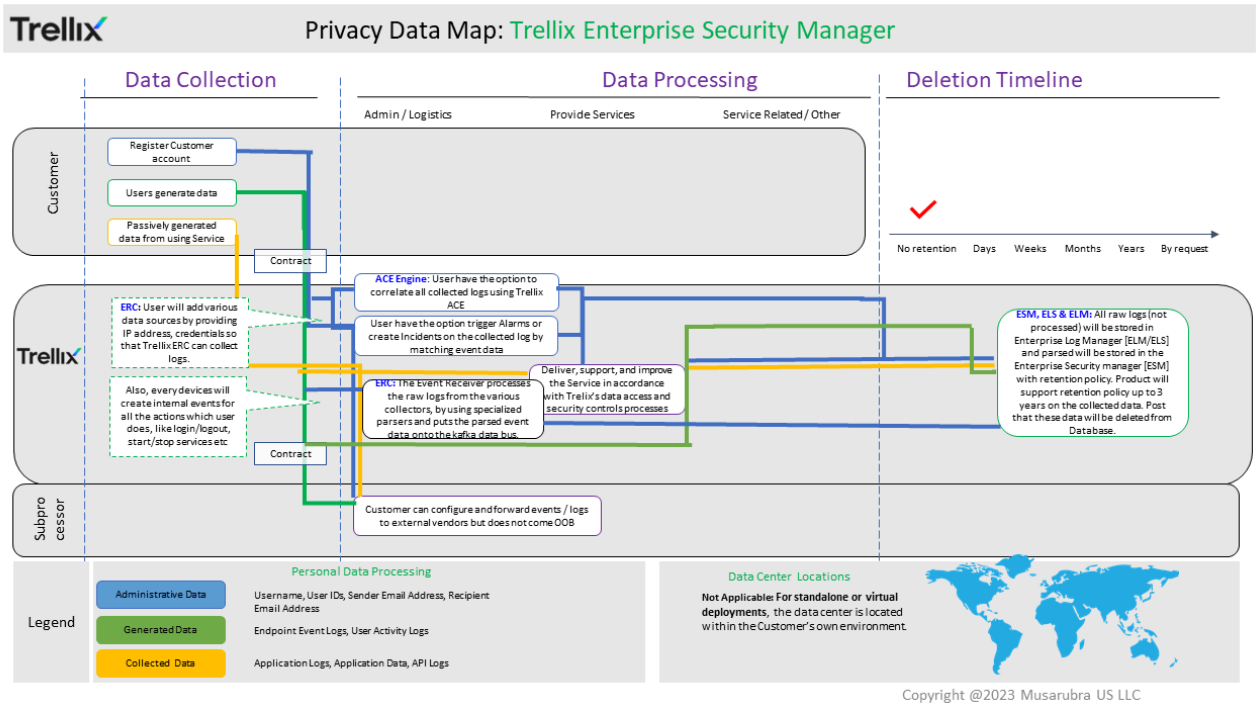
Table 4. Access Control

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	No default access. Access can be granted to Trellix by the

		Customer for debugging of Customer/operational data in the event of an escalation.
Generated Data	Customer	Analysis of User/Systems involved in violations, compliance, and reporting.
	Trellix	No default access. Access can be granted to Trellix by the Customer for debugging of Customer/operational data in the event of an escalation.
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 – Windows.
	Trellix	No default access. Access can be granted to Trellix by the Customer for debugging of Customer/operational data in the event of an escalation.

Trellix Enterprise Security Manager (ESM) 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 ESM 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 the personal data processed by ESM 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 ESM, 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	Duration of subscription contract	To administer the service
Generated Data*	Not applicable	Not applicable
Collected Data*	Not applicable	Not applicable

***Each customer determines how to retain their own data, which can be dictated by compliance requirements or internal policies. Customers choose where to store their data and they define how long to store their data. When it is necessary for Trellix's Support team to collect data, data retention periods are added, and any data collected is encrypted when at rest.

Personal Data Security

Files stored on or processed by Trellix's systems are secured with state-of-the-art technologies, and Trellix operates rigorous technical and organizational security controls designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

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 the global and regional ESM 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 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.

