Trellix Privacy Data Sheet We bring security to life.

Trellix Endpoint Security (HX)

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

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

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

Product Overview

Adaptive security requires monitoring of all threat vectors, including fast, accurate assessments of potential cyberattacks tracked to endpoint activity. Trellix HX allows Customers to detect, analyze, and respond to targeted cyberattacks and zero-day exploits located at the endpoint. Trellix HX processes alerts from Trellix's Indicators of Compromise (IOC), Exploit Guard (EXG), Anti-Virus (AV) and MalwareGuard (MG) technologies.

Armed with this intelligence, HX monitors activity on each endpoint host, collecting real-time, exploit, and malware data from events occurring on the endpoint, and identifying activity that matches the real-time indicator rules and Trellix's exploit and malware intelligence.

[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."

Using Endpoint Security (HX) Customers can continuously monitor endpoints for advanced malware and indicators of compromise (IOCs) that routinely bypass signature-based and defense-in-depth security systems.

Trellix HX automates tasks to:

- Search for advanced attackers and advanced persistent threats (APTs)
- Investigate alerts from network devices, automatically creating IOCs and alert users
- Extend Trellix detection services seamlessly to your endpoints
- Use Agent Anywhere technology to analyze remote endpoints outside the corporate network, regardless of their Internet connection type
- Acquire files, data, and triage collections from endpoints and analyze these collections
- Confirm whether alerts seen on the network in fact compromise endpoints
- Contain endpoints, isolating devices when they become compromised

Trellix HX defends against today's cyberattacks by using a defense-in-depth model. The modular architecture of HX unites default engines and downloadable modules to protect, detect, respond, and manage endpoint security.

Trellix HX includes the following security modules:

- **AMSI** - Monitors, detects, and blocks suspicious scripts using the AMSI interface and generates alerts when malicious scripts are found.
- **Anti-Malware Scan Reports** - Generates scan summary reports for Malware Protection.
- **API Documentation** - Provides access to information about endpoints, acquisitions, alerts, source alerts, conditions, indicators, and containment.
- **Deny List** - Enables a Customer's Security Administrator to alert, block or quarantine files based on hash or a file path list.
- **Agent Console** - This module provides insights into the quarantined items, detected malware, server scheduled scan summary events, and agent version information.
- **Enricher** – Customers gain additional context about alerts within their environment through intelligence about a file, event, or alert displayed in the Endpoint Security Web UI.
- **Event Streamer** - Sends Windows event log data and the contents of various Windows server log files to services supporting the Syslog protocol.
- **Host Management** - Allows Customers to view the state of host endpoints running Endpoint Security.
- **Host Remediation** – Allows Customers to connect an existing Endpoint Security Server to agent endpoints using mutual TLS v1.2 and AEAD mode cipher. No additional firewall rules or ports are required for the module to be able to perform normal operations.
- **IOC Streaming** – Forwards activity events from the Endpoint Security Server to Trellix Helix. The endpoint selects the events to be forwarded based on the rules received from the Endpoint Security Server.
- **Logon Tracker** - Enables the investigation of lateral movement within Windows and Linux enterprise environments.
- **Process Guard** - Protects endpoints from common credential theft attacks. Process Guard prevents attackers from obtaining access to credential data, or key material.

- **Process Tracker Module** - Recognizes unique process execution events.
- **Server Health** - Enables administrators to monitor critical service failures and identify potential issues in the product.

All modules integrate within the Customer enterprise environment. Each module operates independently, as well as collaboratively and dynamically, to provide several layers of security.

With Trellix HX, Security Operators (SOs) are provided investigation workflows used to determine the root cause of a threat event together with the evidence used to identify both known and unknown threats to provide a targeted remedy. Investigation workflows target the compromised endpoint and dynamically expand the SO's investigation capabilities.

Customers can control the degree of monitoring and data collection available on an endpoint via Customer policy configuration settings.

Combined with other Trellix SaaS offerings (including, for example, Trellix Endpoint Security and Trellix Endpoint Detection and Response), HX 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.

Trellix HX can be implemented as one of three deployments:

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

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

- **Managed deployment of HX** – Deployment occurs within Trellix's instance in Amazon Web Services, Inc. (AWS). Trellix owns the appliance on which the HX instance is running, with an independent AWS instance for each HX subscription.

Please see Trellix Endpoint Security (HX) for additional information related to the Trellix HX solution.

Please also see Trellix ePolicy Orchestrator SaaS (ePO-SaaS) Privacy Data Sheet for additional information.

Personal Data Processing

Trellix HX uses Trellix machine learning technology to proactively and automatically monitor and detect malicious activity and policy violations occurring on the Customer's enterprise endpoints. Trellix's machine learning modules analyze event information, in online and offline modes, from the Customer's enterprise endpoints and determines responses based on file reputation, rules, and reputation thresholds, for both traditional and advanced file-less threats.

Configurations, policies, rules, incidents, threats, and event information in support of an investigation may contain personal information from Customer SecOps team members and enterprise endpoint systems. Trellix will capture information differently depending on the HX deployment version:

- **Standalone deployment of HX:** The solution reads data stored on the Customer's network environment and no data is captured by Trellix.
- **Virtual deployment of HX:** The solution reads data stored on the Customer's network environment and no data is captured by Trellix.
- **Managed deployment of HX:** 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, Trellix HX may process a range of data potentially containing personal information. The table below shows the personal data processed by HX to provide its services and describes why the data is processed.

Table 1. Personal Data Processed by Trellix Endpoint Security - HX

Personal Data Category*	Types of Personal Data Processed	Purpose of Processing
Administrative Data	General identification information: ● Username ● Full Name ● Password ● IP Address(es) ● MAC Address ● Hostname ● Device Serial Number ● Operating System Details ● CPU Information ● Time Zone ● Uptime ● Last Communication Time ● Email Address ● IP Address of User Device ● Browser Information	User access and authorization management.
Generated Data	Incidents / Events: ● File Data Written ● Network Destinations ● DNS Lookups ● Registry Data ● Application Data ● Activity Timestamps ● Network Address Updates Evidence:	Monitoring data: Used to discern suspicious activities from normal activities.

	• All recent process activity on the machine • All browser history • All data on disk • Data within Active Memory	
Collected Data	Configuration Information: • File • Event History • Product Logs • Audit Logs	Monitoring of operations.

***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

Trellix uses its own data centers as well as third-party infrastructure providers to deliver the service globally. HX processes the personal data in Amazon Web Services (AWS) regional clouds located in the United States, Japan, Singapore, India, Australia, Germany, and Canada. 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 West (Oregon)
AWS	AWS East (Virginia)
AWS	Japan (Tokyo)
AWS	Singapore
AWS	India (Mumbai)
AWS	Australia (Sydney)
AWS	Germany (Frankfurt)
AWS	Canada (Central)

Subprocessors

Trellix partners with service providers that act as subprocessors for the HX 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	AWS East (Virginia)
AWS	See Table 1	Hosting	Japan (Tokyo)
AWS	See Table 1	Hosting	Singapore
AWS	See Table 1	Hosting	India (Mumbai)
AWS	See Table 1	Hosting	Australia (Sydney)
AWS	See Table 1	Hosting	Germany (Frankfurt)
AWS	See Table 1	Hosting	Canada (Central)

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).

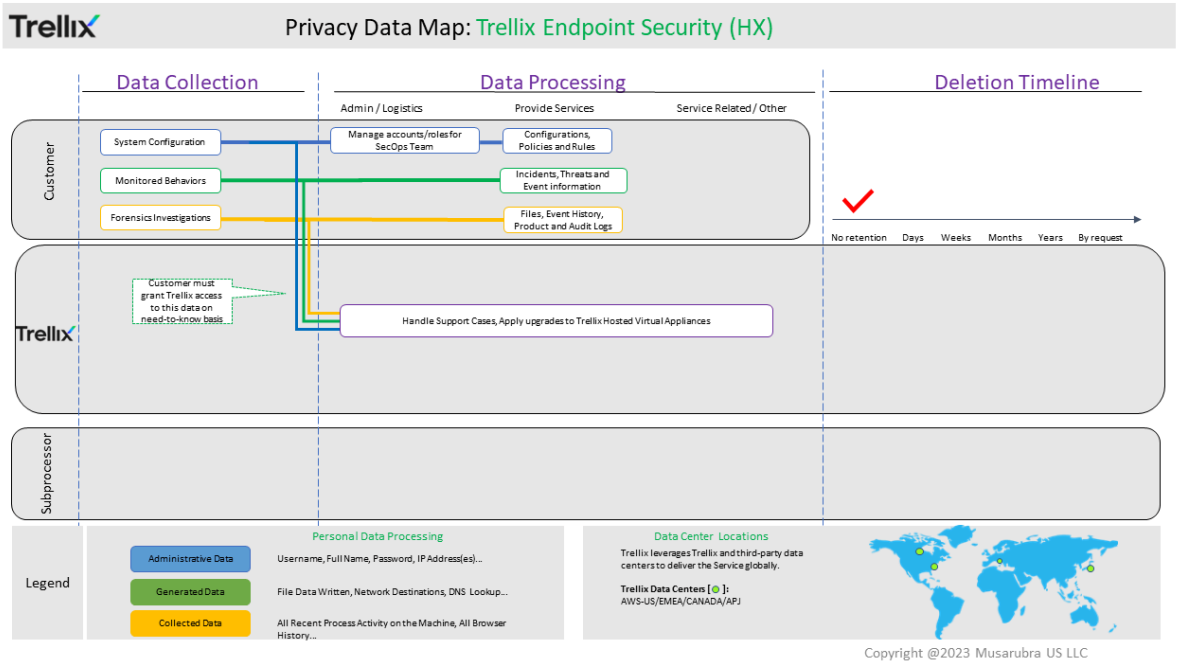
Remote user access by Trellix personnel is performed through a secure virtual private network (VPN) connection that requires multi-factor authentication (MFA). If remote access to production resources is required outside the VPN, then a TLS encrypted connection and MFA are required.

The table below lists the personal data used by Trellix HX 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: System administrators	Administration of access and roles on the appliance. Identification and classification of endpoints monitored within the enterprise.
	Trellix: Customer support staff when granted access, or data is explicitly shared by the Customer.	Analysis during problem escalation.
Generated Data	Customer: Users of the system granted access to analyze threats identified by the system	To discern suspicious activities from normal activities.
	Trellix: Customer support staff when granted access, or data is explicitly shared by the Customer.	Analysis during problem escalation.
Collected Data	Customer: System administrators, local IT support staff.	Monitoring of operations. Analysis during problem escalation.
	Trellix: Customer support staff when granted access, or data is explicitly shared by the Customer.	

Trellix Endpoint Security (HX) - Data Flow Diagram



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 HX 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 HX 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 HX, 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	30 – 60 days (about 2 months)	Grace period upon expiration of license, to allow for renewal without loss of data.
Generated Data	30 – 60 days (about 2 months)	Grace period upon expiration of license, to allow for renewal without loss of data.
Collected Data	30 – 60 days (about 2 months)	Grace period upon expiration of license, to allow for renewal without loss of data.

*** This pertains only to managed deployments of the HX solution in Trellix's instance in AWS. No retention exists for the other deployment modes.**

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.

For managed deployment of the HX service:

HX 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, 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 the global and regional HX 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 that 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.