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

Health Watch

The purpose of this Privacy Data Sheet is to provide customers of Health Watch 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.

Health Watch is a security health check and assessment solution made available by Trellix to companies or persons who obtain a Trellix Health Watch subscription.

Trellix will process personal data from Health Watch 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 Health Watch to provide its functionality.

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

Product Overview

The Trellix Health Watch solution is a high-value service that helps ensure a Trellix customer's security investment is optimized to help reduce threats, reduce operational costs, and to best leverage innovative technology. Health Watch utilizes a portal, proprietary software tools, and Professional Services consultants to collect and analyze data, assign risk and scores, generate action plans, and deliver a consistent, high-quality report to our customers.

Please also see Solution Services for additional information related to the Trellix Health Watch solution.

[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."

Personal Data Processing

Customer data is routinely captured from the customer's environment as part of the Health Watch service. The captured data contains information about Trellix systems including system names, settings, configurations, policies and rules, hardware, and log information produced by Trellix products. Trellix Health Watch can be configured by the customer to meet the customer's needs. As a result, Health Watch may process a range of data potentially containing personal data. The table below shows the personal data processed by Health Watch to provide its services and describes why the data is processed.

Table 1. Personal Data Processed by Health Watch

Personal Data Category	Types of Personal Data Processed	Purpose of Processing
Health Watch Portal Account/Contact Information	General identification information: ● Customer name ● Email address	● Activation of service ● Authentication
Health Watch Collected Information from Trellix Products	General identification information: ● Employee name ● Email address ● Phone number Incidents/Events: ● Device names ● Device IDs ● Hostnames ● IP (Internet Protocol) addresses of servers databases, endpoint devices	● Managing accounts within Trellix products ● Report findings from the Health Watch analysis and attribute such findings to specific devices, servers, endpoints, etc.

Data Center Locations

Trellix uses its own data centers and third-party infrastructure providers to deliver the service globally. Heath Watch processes the personal data in Trellix's instance in AWS (Amazon Web Services) regional clouds located in the United States. 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.

The Health Watch system hosted by AWS uses AWS for DNS, firewall, gateway, load balancer, containers, database storage, encryption, monitoring, and auditing. Additionally, the AWS environment is actively monitored real-time by Trellix's SOC (Security Operations Centre) personnel who can enable blocking and disabling of traffic to the system in the event of unauthorized intrusion or breach.

Table 2. Data Center Locations

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

Subprocessors

Trellix partners with service providers that act as subprocessors for the Health Watch service and contract 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 Processed	Service Type	Location of Data Center
AWS	All	Hosting and storage	AWS West (Oregon)

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 Data 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 responsible for deciding who will be granted access to them. 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.

All external and internal user accounts are required to update their passwords every 90 days. Failure to update your password within 90 days will deactivate the account.

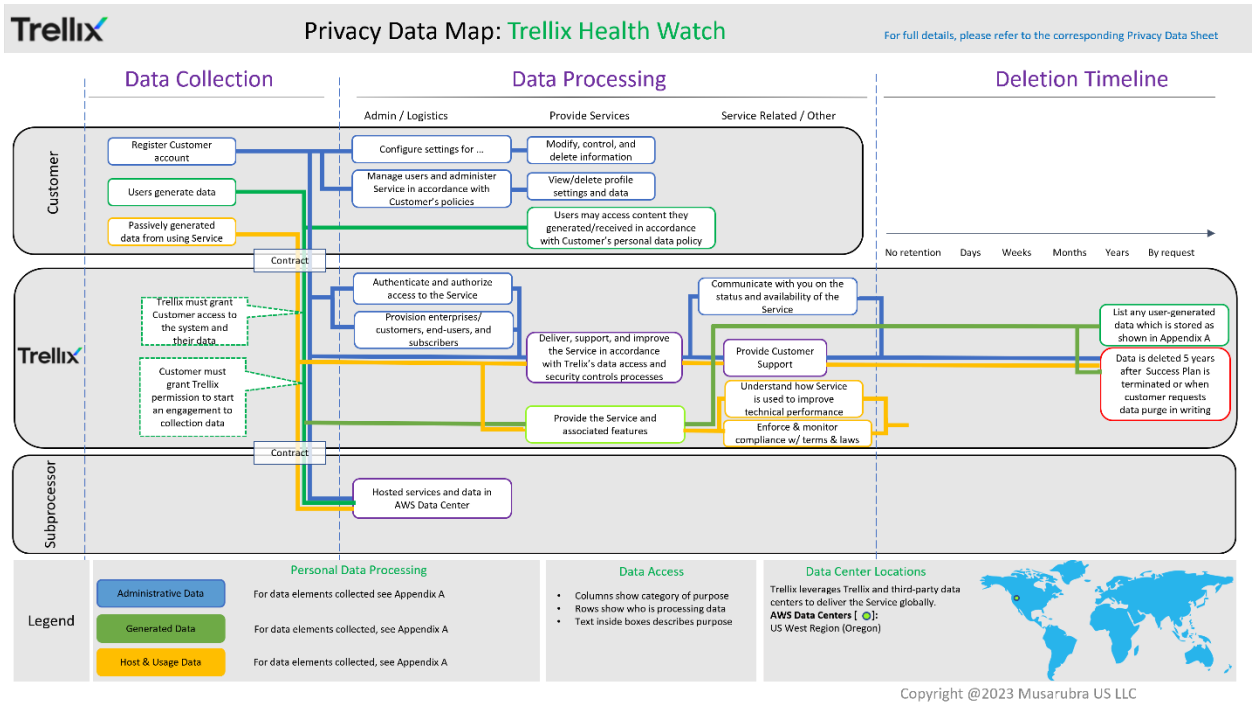
The table below lists the personal data used by Health Watch to carry out the service, who can access that data, and why.

Table 4. Access Control

Personal Data Category	Who has access	Purpose of the access
Health Watch Portal Account/Contact Information	**Customer** 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.	Account management
	Trellix Remote access by Trellix personnel is performed through a secure virtual private network (VPN) connection that requires multi-factor authentication (MFA).	Account management, authentication
Health Watch Collected Information from Trellix Products	**Customer** 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.	View Health Watch results
	Trellix Remote access by Trellix personnel is performed through a secure virtual private network (VPN) connection that requires multi-factor authentication (MFA).	View and edit Health Watch results

Health Watch 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, policy enforcement, access controls, logging capabilities, individual rights processing and cross-border data transfer mechanisms.

Customers control whether the Health Watch 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 Deletion and Retention

As part of the Trellix Health Watch service, the collection tool must be run in the customer environment and can only be used during an active engagement. An engagement is activated by the customer completing and accepting registration to the portal and the engagement.

Because certain features of Health Watch utilize data from prior Health Watch Reports (i.e., identification of changes to the environment, findings trends, scoring trends, and anonymized industry trends), data in

the Health Watch database will be automatically retained by Trellix. Health Watch data is retained for 5 years after a customer terminates a Trellix Success Plan.

The table below lists the personal data used by Health Watch, the length of time that data needs to be retained, why we retain it, and location of storage.

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 HealthWatch@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
Health Watch Portal Account/Contact Information	5 years after a customer terminates a Trellix Success Plan or until a purge request is submitted	Account management, authentication
Health Watch Collected Information from Trellix Products	5 years after a customer terminates a Trellix Success Plan or until a purge request is submitted	Data trends, improvements/worsening of security posture

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.

Health Watch 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

The Health Watch database is backed up incrementally throughout the day and fully backed up daily. Database access is restricted to the Health Watch administrators.

Table 6. Personal Data Security

Personal Data Category	Type of Personal Data	Security Controls and Measures
Health Watch Portal Account/Contact Information	See Table 1	Encrypted in transit and at rest
Health Watch Collected Information from Trellix Products	See Table 1	Encrypted in transit and at rest

Compliance with Privacy Requirements

Trellix is committed to protecting personal data processed in the global and regional Health Watch 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 (888) 847-8766

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.