Trellix Privacy Data Sheet We bring security to life.

Trellix Cloud Workload Security (CWS)

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

CWS 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 CWS subscription.

Trellix will process personal data from CWS 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 CWS in order to provide its functionality.

This Privacy Datasheet is a supplement to the Trellix Website Privacy Notice.

Product Overview

Trellix CWS enables automatic discovery, management, and enforcement of security tasks and policies across Trellix Customers' entire enterprise endpoint system and provides automatic integration and configuration with private, public, and/or multicloud offerings, including Amazon Web Services (AWS), Microsoft Azure, and VMware vCenter.

With Trellix CWS, Customers' Security Operators Administrators (SecOps Admins) can visualize the security posture of all distributed endpoints across the Customer's entire enterprise using Trellix ePolicy Orchestrator's (ePO) command center and can access the CWS service through a configurable user interface for the ePO On-Prem service.

[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 CWS offers improved visibility and control to address the unique requirements of public cloud server security. It detects and imports virtual infrastructure details, security groups, and virtual networks to the Trellix ePO server. It provides control over cloud infrastructure and insights into threat information across clouds. It also offers infrastructure visibility and security alerts so that you can quickly assess security issues and take immediate action.

Combined with other Trellix cybersecurity offerings (including, for example, Trellix ePolicy Orchestrator (ePO On-Prem)), Trellix CSW enables monitoring on the full spectrum of new and emerging cyber threats in real time, across all vectors—file, web, message, and network.

Trellix CWS provides protection that makes it possible for a single, automated policy to effectively secure your workloads as they transition through your virtual private, public, and multicloud environments, enabling operational excellence for Trellix Customers' cybersecurity teams.

The CWS solution ensures that Customers maintain the highest quality network security while taking advantage of the cloud. It covers multiple protection technologies, simplifies security management, and prevents cyber threats from impacting Trellix Customers' core business functions.

Trellix CWS includes the following security features:

- **Automated Discovery** – Enables discovery of elastic workload instances and Docker containers across Amazon Web Services (AWS), Microsoft Azure, OpenStack, and VMware environments. Customers gain a centralized and complete view across environments.
- **Consolidate Events** – Allows organizations to use a single interface to manage numerous countermeasure technologies for both on-premises and cloud environments. Permits integration into additional third-party countermeasure technologies including AWS Guard Duty, Trellix Policy Auditor, and Trellix Intrusion Prevention System.
- **Enforcement of Network Security Group Policies** – Permits users and administrators to create baseline security group policies and audit the policies that are running on the workloads against the baselines.
- **Cloud-Native Build Support** – Consolidates management of multiple public and private clouds in a single management console, including AWS, EC2, Microsoft Azure Virtual Machines, OpenStack, and VMware Vcenter.
- **Simple, Centralized Management –** Provides a single console for consistent security policy and centralized management of multicloud environments across servers, virtual servers, and cloud workloads. Administrators can create multiple role-based permissions in Trellix ePO On-Prem.
- **Auto-Remediation –** Automatically quarantines a system that is not protected by Trellix ePO On-Prem security policies and is found to contain malware or virus.
- **Adaptive Threat Protection** – Integrates comprehensive countermeasures, including machine learning, application containment, virtual machine-optimized anti-malware, whitelisting, file integrity monitoring, and micro-segmentation that protects workloads from ransomware and targeted attacks. Advanced threat protection defeats attacks by applying machine learning techniques to convict malicious payloads based on code attributes and behavior.
- **Application Control -** Prevents both known and unknown attacks by allowing only trusted applications to run, while blocking unauthorized payloads.

- **File Integrity Monitoring (FIM) -** Continuously monitors your system files and directories to ensure they have not been compromised by malware, hackers, or malicious insiders.

CWS is only implemented as an ePO On - Prem deployment: Customers use tenant credentials (Trellix Agent) for ePO On - Prem to create/deploy, manage, and enforce security policies. Customers can use the queries and dashboards options to track detections, activities, and status of their enterprise endpoint infrastructure within their organization.

Please see Trellix Cloud Workload Security for additional information related to the Trellix Cloud Workload Security solution.

Please see Trellix ePolicy Orchestrator on Premise (ePO On-Prem) Privacy Data Sheets for additional information.

Personal Data Processing

Trellix CWS provides visibility into and security for the Customer's cloud infrastructure. The captured information is stored locally in Trellix ePO On-Prem within the Customer's environment.

Trellix ePO On - Prem deployment: The captured event information is sent automatically to Trellix Agent by way of SSL/HTTPS connection to ePO On-Prem server/database present within the Customer's environment. As a result, CWS may process a range of data potentially containing personal information. The table below shows the personal data processed by CWS to provide its services and describes why the data is processed.

Table 1. Personal Data Processed by Trellix Cloud Workload Security

Personal Data Category	Types of Personal Data Processed	Purpose of Processing
Administration Data	General identification information: ● Device Name ● IP Address ● Mac Address ● Trellix Agent GUID ● System Tag ● Cloud Credentials	Used to manage business operations ensuring compliance, provide reporting, and facilitate troubleshooting.
Generated Data	Incidents / Events: ● Instances Security State ● Security Software Installed Status ● Network Security Status Evidence: ● Display the Status in CWS UI and Allow the Admin to act	Endpoint management, compliance, auditing, and threat analysis.

Collected Data	Configuration information: ● Product Logs ● Active Directory Username	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

ePolicy Orchestrator on Premise (ePO On - Prem) deployment, the data center is located within the Customer's network environment.

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 CWS 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 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.

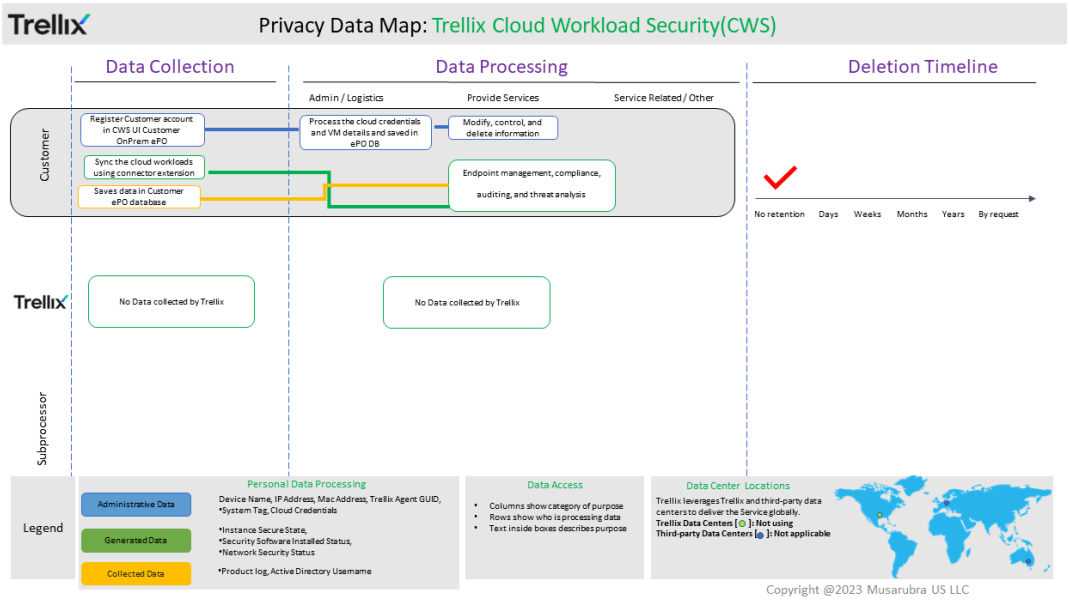
The table below lists the personal data used by CWS to carry out the service, who can access that data, and why.

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.
	Trellix:	No default access.
Generated Data	Customer:	To check the status of VMs security posture.
	Trellix:	No default access.
Collected Data	Customer:	To check the health status of the CWS service.
	Trellix:	No default access. Access can be granted to Trellix by the Customer.

Trellix Cloud Workload Security 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 CWS 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 CWS to a third-party data store. 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 CWS, 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	Not Applicable	Not Applicable
Generated Data	Not Applicable	Not Applicable
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.

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 certifications are available upon request.

Compliance with Privacy Requirements

Trellix is committed to protecting personal data processed in the global and regional CWS 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.