Trellix Privacy Data Sheet We bring security to life.

Trellix Application Control - SaaS (AC - SaaS)

The purpose of this Privacy Data Sheet is to provide Customers of Trellix AC - SaaS 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 AC - SaaS 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 AC - SaaS subscription.

Trellix will process personal data from AC - SaaS 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 Trellix AC - SaaS to provide its functionality.

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

Product Overview

Trellix AC - SaaS* is a Trellix security solution that blocks unauthorized applications from running on Customer enterprise endpoints, including servers, corporate desktops, and fixed-function devices. Application Control protects Customer enterprises against malware attacks before they occur by proactively verifying the applications that run on enterprise devices. Application Control uses dynamic allowlisting to help guarantee that only trusted applications run on servers, devices, and desktops. Application Control eliminates the need for Security Operations Administrator (SecOps Admin) to manually maintain lists of approved applications.

This privacy data sheet describes Application Control - SaaS (AC-SaaS) only. Change Control - SaaS will be a part of a future software release.

Application Control automates tasks to:

- Prevent malicious, untrusted, or unwanted software from executing;

[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."

- Identify trusted software and grants it authorization to run;
- Block users from introducing software that poses a risk to Customer enterprise systems; and
- Tracks changes happening in the system.

Trellix Application Control includes the following security features:

- **Dynamic allowlisting:** Manages allow lists in a secure and dynamic way. Application Control groups executables (binaries, libraries, and drivers) across the Customer's enterprise;
- **Protection against cyber threats:** Extends coverage to executable files, libraries, drivers, Java applications, ActiveX controls, and scripts for greater control over application components. It also locks down protected endpoints against threats and unwanted changes, with no file system scanning or other periodic activity that might impact system performance;
- **Advanced memory protection:** Grants multiple memory-protection techniques to prevent zero-day attacks. Memory-protection techniques provide extra protection over the protection from native Windows features or signature-based buffer overflow protection products;
- **Knowledge acquisition:** Enables discovery of policies for dynamic desktop environments without enforcing allowlist lockdown. This mode helps SecOps Admins deploy the software in pre-production environments without affecting the operation of existing applications;
- **Reputation-based execution:** Integrates with a reputation source to receive reputation information for files and certificates, depending on a verdict. Application Control allows or bans the execution and software installation;
- **Centralized management:** Application Control integrates with Trellix ePO - SaaS for consolidated and centralized management, and a global view of enterprise security from a single console.

Trellix AC - SaaS is offered as:

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

Please see, Trellix Application and Change Control for additional information related to the Trellix AC - SaaS solution.

Please also see, Trellix ePolicy Orchestrator - SaaS for additional information related to the Trellix ePO - SaaS solution.

Personal Data Processing

Trellix AC - SaaS enables SecOps admins to manage all endpoints, deploy policies, create rules, add certificates, manage data inventory, monitor activities, and approve requests.

Trellix AC - SaaS captures data to perform monitoring and detection of cyber threats across the Customer's entire enterprise.

- **Trellix ePolicy Orchestrator - SaaS (ePO - SaaS) deployment:** The captured event information is sent via Trellix Agent to Trellix ePolicy Orchestrator (ePO - SaaS) by way of SSL/HTTPS connection to Trellix ePolicy Orchestrator (ePO On - SaaS) server/database.

As a result, Trellix AC - SaaS may process a range of data potentially containing personal information.

The table below shows the personal data processed by Trellix AC - SaaS to provide its services and describes why the data is processed.

Table 1. Personal Data Processed by Trellix Application Control - SaaS

Personal Data Category	Types of Personal Data Processed	Purpose of Processing
Administrative Data	General Identification Information: ● User Name ● Device Name ● IP Address ● Mac Address ● Trellix Agent GUID ● OS Name ● Product Name ● EPO GUID ● Binary Hash ● SHA1s of C-Certs ● Product Version	Used to manage business operations, ensuring compliance, provide reporting, and facilitate troubleshooting.
Generated Data	Incidents / Events: ● Event Type ● Vendor Name ● Application Name ● Application Binary Cert Details Evidence: ● File Name ● File Path ● File Version ● File Size	Used for system management, threat investigation and audit logging.
Collected Data	Configuration Information: ● System Tag ● Product Logs	Troubleshooting through Trellix support.

****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

Trellix uses its own data centers as well as third-party infrastructure providers to deliver the service globally. Trellix AC - SaaS processes the personal data in Trellix's instance in Amazon Web Services, Inc. (AWS) regional clouds located in the United States, Australia, Canada, India, Germany and Singapore. 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 modified by a system administrator, traffic in certain countries will be directed to a designated compute location.

Table 2. Data Center Locations

Data Center Provider	Data Center Location
AWS	AWS West (Oregon)
AWS	Australia (Sydney)
AWS	India (Mumbai)
AWS	Germany (Frankfurt)
AWS	Singapore

Subprocessors

Trellix partners with service providers that act as subprocessors for the Trellix AC - SaaS 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	Australia (Sydney)
AWS	See Table 1	Hosting	India (Mumbai)
AWS	See Table 1	Hosting	Germany (Frankfurt)
AWS	See Table 1	Hosting	Singapore
Okta	See Table 1	Authentication	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 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.

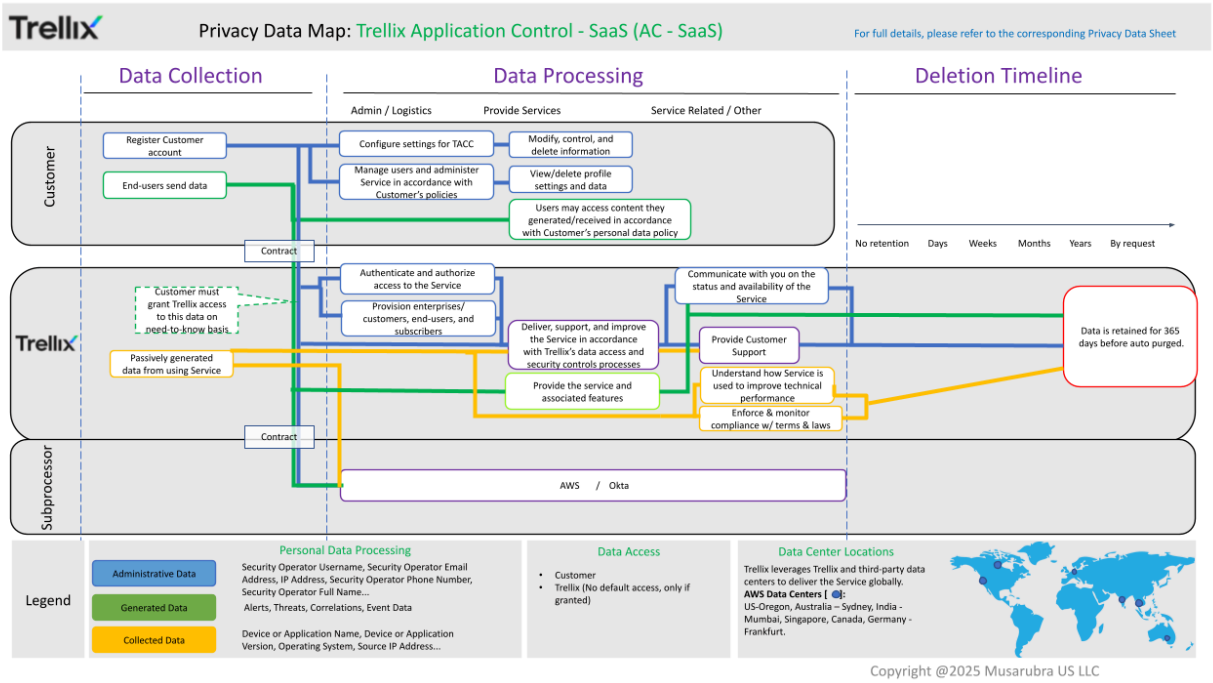
The table below lists the personal data used by Trellix AC - SaaS to carry out the service, who can access that data, and why.

Table 4. Access Control

Personal Data Category	Who has access	Purpose of the access
Administrative Data	Customer	Administration of access and roles on the managed node. Identification and classification of endpoints monitored within the enterprise.
	Trellix	Analysis during problem escalation.
Generated Data	Customer	Identify suspicious activities from normal activities and alert the Customer.
	Trellix	Analysis associated with escalations.
Collected Data	Customer	Monitoring of operations.
	Trellix	Analysis associated with escalations.

Trellix Application and Change Control - 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 Trellix AC - SaaS 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 Trellix AC - SaaS 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., 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 Trellix AC - SaaS, 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	Data is retained for 365 days.	Compliance, reporting, troubleshooting.
Generated Data	Data is retained for 365 days.	Compliance, reporting.
Collected Data	Data is retained for 365 days.	System integrations.

***Deletion of data may also occur upon Customer request or at the end of the subscription.

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.

Trellix AC - SaaS uses a secure portal hosted by AWS to store product 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 certifications are available upon request.

Compliance with Privacy Requirements

Trellix is committed to protecting personal data processed in the global and regional Trellix AC - SaaS 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, Shibuya-ku, Tokyo 150-0043

About This Privacy 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.