Trellix Privacy Data Sheet We bring security to life.

Trellix Application and Change Control (TACC) for Windows and Linux

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

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

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

Product Overview

Trellix ACC – Windows is a Trellix security solution that combines Application and Change Control to block 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.

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
- Track the changes happening in the system.

Trellix Change Control monitors and prevents unauthorized changes to critical system files, directories, and configurations while implementing new policies and compliance measures. Change Control tracks changes to files and registry keys in real time and it identifies who made changes to which files. Change Control blocks change activities in server environments and allows Customers to write-protect and read-protect critical files from unauthorized tampering. A Customers SecOps Admin defines trusted programs or users to allow updates to protected files and registry keys. A change is allowed only if it is applied according to the Customer's configuration policies.

Change Control automates tasks to:

- Detect, track, and validate changes in real time;
- Prevent changes using protection rules; and
- Enforce approved change policies.

As a combined Application and Change Control offering, Trellix ACC gives SecOps Admins control over all Customer endpoints to help enforce rules and policy compliance. Trellix ACC leverages a dynamic trust model and innovative security features to prevent advanced persistent threats (APT) without requiring signature updates. It helps guarantee protection without impacting productivity.

Used in combination with other Trellix offerings (including, for example, Trellix Global Threat Intelligence (Trellix GTI) and Trellix Threat Intelligence Exchange (Trellix TIE)), Trellix Application and Change Control leverages the cloud to monitor and act on the full spectrum of new and emerging cyberthreats in real time, across all vectors—file, web, message, and network.

Trellix Application and Change 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;
    - Note that this feature is available only in a Trellix ePO-On-prem deployment;
- **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;
    - Note that this feature is available only in a Trellix ePO-On-prem deployment.

- **Centralized management:** Application Control integrates with Trellix ePO - On-prem for consolidated and centralized management, and a global view of enterprise security from a single console;
    - Note that this feature is available only in a Trellix ePO-On-prem deployment.
- **Write protection:** Uses write protection rules to prevent users from creating and changing files, directories, and registry keys.
- **Read protection:** Read protection rules prevent users from reading the content of specified files, directories, and volumes;
- **Real-time monitoring:** Change Control monitors file and registry changes in real time, eliminating need for multiple scans on endpoints to identify change violations;
- **Content change tracking:** Change Control tracks content and attribute changes for files and includes special alerting mechanisms to instantly notify the SecOps Admin of critical changes.

Trellix ACC can be implemented as one of two deployments:

- **Standalone deployment of Trellix ACC** - Available to install by the Customer's systems administrator to configure settings through the interface; or

- **Managed deployment of Trellix ACC** - Available via **Trellix ePolicy Orchestrator on Premise (ePO On - Prem):** 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 managed Windows systems within their organization.

Please see Trellix Application and Change Control for additional information related to the Trellix Application and Change Control solution.

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

Personal Data Processing

Trellix ACC solution automatically monitors and detects malicious activity and policy violations occurring on the Customer's enterprise endpoints. Trellix ACC allows SecOps Admins to manage all endpoints, deploy policies, create rules, add certificates, manage data inventory, monitor activities, and approve requests.

Trellix ACC captures data to perform monitoring and detection of cyber threats across the Customer's entire enterprise. Trellix will capture information differently depending on the ACC deployment version:

- **Standalone deployment of Trellix ACC:** The solution reads data stored on the Customer's enterprise endpoints and no data is captured by Trellix.
- **Trellix ePolicy Orchestrator on Premise (ePO On - Prem) deployment:** The captured event information is sent automatically to Trellix Agent by way of SSL/HTTPS connection to Trellix ePolicy Orchestrator (ePO On - Prem) server/database present on the Customer's premises.

As a result, Trellix ACC may process a range of data potentially containing personal information.

The table below shows the personal data processed by ACC to provide its services and describes why the data is processed.

Table 1. Personal Data Processed by Trellix Application and Change Control

Personal Data Category	Types of Personal Data Processed	Purpose of Processing
Administrative Data	General identification information: • Username • Device Name • IP address • Mac address • Trellix agent GUID • OS Name	It is captured to identify who is executing the unauthorized applications and who should be contracted further to rectify the issue. This data is also captured to identify which system is not protected or protected, so that the issue can be rectified if any exist.
Generated Data	• Product Name • EPO GUID • Binary hash • SHA1s of certs • Product version • Event type • File Name • File path • File version • File Size • Vendor Name • Application Name • Application Binary cert details	This information is sent as part of the GTI Request. GTI Requests are performed to find the reputation of applications and to send telemetry data. Based on the reputation Trellix ACC can make decisions allowing or denying the execution of applications.
Collected Data	Configuration Information: • System Tag • Product Logs	This is used for finding the task status and troubleshooting the issue through Trellix support.

***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

For standalone deployment, all data is stored on the Customer's enterprise endpoints and no data centers are utilized by the service.

For Trellix managed deployment, Trellix processes personal data via Trellix ePO On-Prem located within the Customer's 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 ACC 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 TACC to carry out the service, who can access that data, and why.

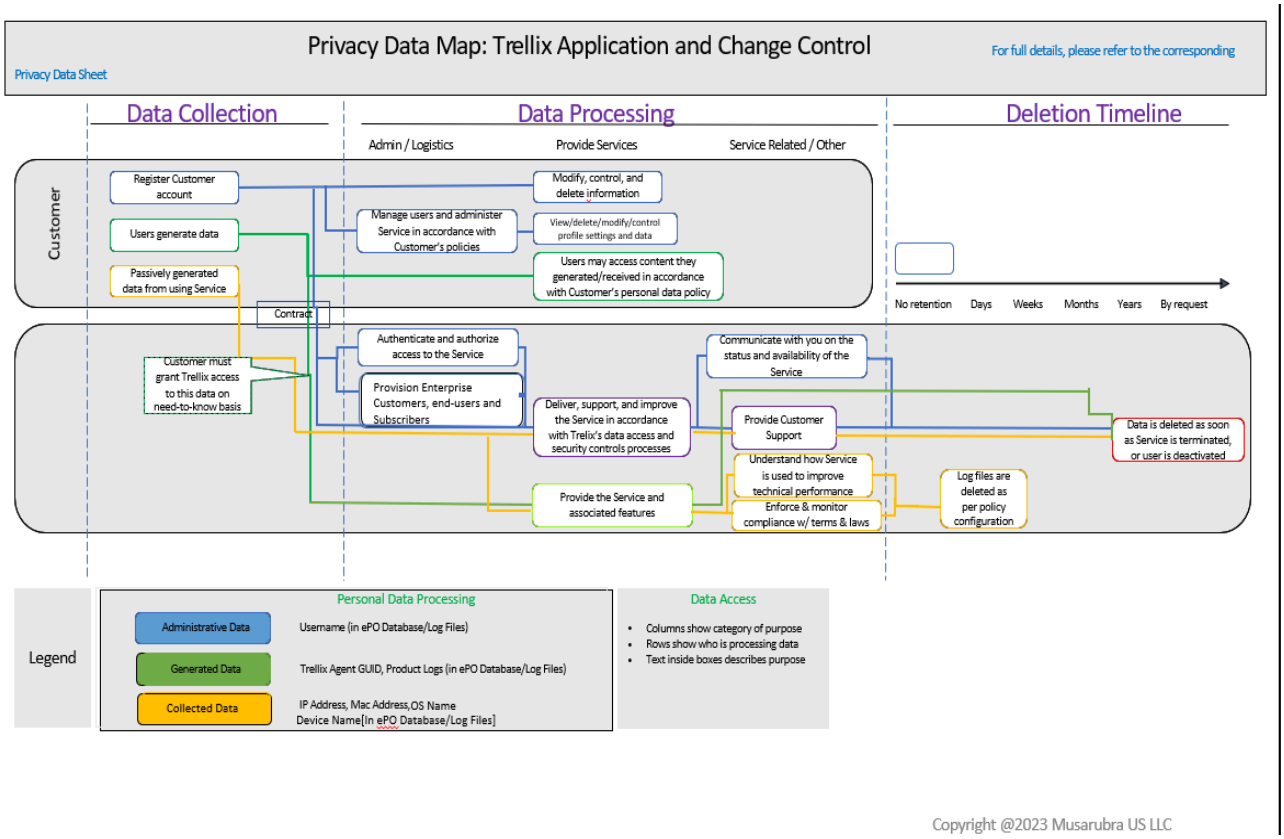
Table 4. Access Control

Personal Data Category	Who has access	Purpose of the access
Administrative Data	Customer	Once a solid core event is detected, this information is collected locally and also sent to the on-prem ePO. These events are collected to notify the Customer about the unauthorized execution and file operation. This category of data can be used by the Customer for further system audits.
	Trellix	No default access. This category of data can be captured and sent to Trellix Technical Support to assist Customers in troubleshooting or debugging Trellix product issues.
Generated Data	Customer	Used to determine the reputation of applications which can be used by the product to allow or deny execution.
	Trellix	No default access. This category of data can be captured and sent to Trellix Technical Support to assist Customers in troubleshooting or debugging Trellix product issues.
Collected Data	Customer	This is used for finding the task status and troubleshooting the issue through Trellix support.
	Trellix	No default access. This category of data can be captured and sent to Trellix Technical Support to assist Customers in

		troubleshooting or debugging Trellix product issues.

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 the TACC 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 TACC 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 ACC, 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 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 certifications are available upon request.

Compliance with Privacy Requirements

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