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

Trellix Intelligent Virtual Execution (IVX) - Cloud

The purpose of this Privacy Data Sheet is to provide Customers of Trellix IVX - Cloud 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 IVX - Cloud is a solution which protects servers, computer systems, laptops and tablets against known and unknown threats like malware, suspicious communications, unsafe websites and files, which is made available by Trellix to companies or persons who obtain a IVX - Cloud subscription.

Trellix will process personal data from IVX - Cloud 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 IVX - Cloud to provide its functionality.

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

Product Overview

Trellix IVX - Cloud is a signatureless, dynamic analysis engine that inspects suspicious network traffic to identify attacks that evade traditional signature and policy-based defenses. It also delivers flexible file and content analysis capabilities to identify malicious behavior.

With IVX - Cloud, Customers can protectively submit files, URLs, emails, attachments, and other digital aspects of a collaborative workflow to help ensure they are protected against today's cyberthreats—whether they exploit Microsoft Windows, Apple OS X, Linux, or other application-level vulnerabilities.

Trellix IVX Cloud compares file submissions across the Customer's entire enterprise system and leverages the Trellix Intelligent Virtual Execution (IVX) detection engine and multiple dynamic machine learning, AI,

[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."

correlation engines and the MITRE ATTACK framework to quickly reach a verdict on submitted files. Trellix also determines the possibility of secondary or combinatory effects across multiple phases of the attack lifecycle to discover never-before-seen exploits and malware.

Trellix IVX - Cloud consists of the following security features:

- Detection and prevention of known and unknown malware;
- Integration with all major cloud storage solutions and many web applications;
- Protection of multiple operating systems, including Windows, Mac, and Linux;
- Compiles in-depth analysis details, including MITRE ATT&CK mapping, extracted objects, IOCs, and more;
- Supports plug-ins for browsers and cloud storage;
- Delivers contextual analysis of detected malware in JSON format.
-

Please also see Trellix IVX - Cloud for additional information related to the Trellix IVX - Cloud solution.

Personal Data Processing

When a file is uploaded or delivered to a collaboration tool, shared workspace and/or a cloud application, Trellix IVX - Cloud analyzes the file to identify malware and/or other suspicious activity indicators. If the file is determined to be potentially malicious, it is identified, renamed, sent to a quarantine file, and/or denoted as a potential threat.

Once file identification is performed and analysis of the file is assessed, then a verdict assigning the file as malicious or safe is determined based on internal and global threat intelligence. Once a verdict identifies the nature of a file as malicious, an alert is carried out, notifying the organization that the file needs attention.

With IVX – Cloud, Customers also get supporting contextual detail, including file, registry, process, and network changes, as well as MITRE ATT&CK mapping and other relevant findings from Trellix's continually updated proprietary Trellix Dynamic Threat Intelligence.

IVX - Cloud is available to Customer systems through an API and can easily integrate into the Customer's security operations workflow, SIEM analytics, data repositories, customer web applications, and more.

Personal data elements are captured as part of the IVX console interface and API. For example, IVX - Cloud captures the source IP of the sample submitted, the sender geo location, the source of the sample, sample path, owner of the file, file size, file name, and/or any hashed data. IVX - Cloud also captures additional administrative information captured to access the service.

As a result, IVX - Cloud may process a range of data potentially containing personal information. The table below shows the personal data processed by IVX - Cloud to provide its services and describes why the data is processed.

Table 1. Personal Data Processed by Trellix IVX - Cloud

Personal Data Category*	Types of Personal Data Processed	Purpose of Processing

Administrative Data	General identification information: ● Email ID ● First Name ● Last Name ● Company Name ● Company Address ● Company Size ● Phone Number ● Company Website (Optional)	Used to manage business operations ensuring compliance, provide reporting, and facilitate troubleshooting.
Generated Data	Internet protocol (IP) address / contents: ● IP Source Address Submitted sample data contents: (Malicious and Non-Malicious) Additional context submitted by user which may include server name, submitter name/email, etc.: ● IP Address of Sender Source ● Source of sample (API, Web, Enterprise Applications) Connector data: ● Source IP ● File Owner ● File Path ● File Size ● File Hash ● URL ● Connector Type (Box, Teams, Slack, Salesforce, WebEx etc.)	Used for auditing and threat analysis.
Collected Data	Configuration information: ● YARA custom rules ● Riskware policy ● Guest Image customizations (e.g., Domain, Hostname, Username, File & Folder names)	Used to Integrate with user 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

Trellix uses its own data centers as well as third-party infrastructure providers to deliver the service globally. IVX - Cloud processes the personal data in Trellix's instance in Amazon Web Services, Inc. (AWS) regional clouds located in the United States and Germany. 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 East (Virginia)
AWS	Germany (Frankfurt)

Subprocessors

Trellix partners with service providers that act as subprocessors for the IVX - Cloud 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 East (Virginia)
AWS	See Table 1	Hosting	Germany (Frankfurt)
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 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 IVX - Cloud to carry out the service, who can access that data, and why.

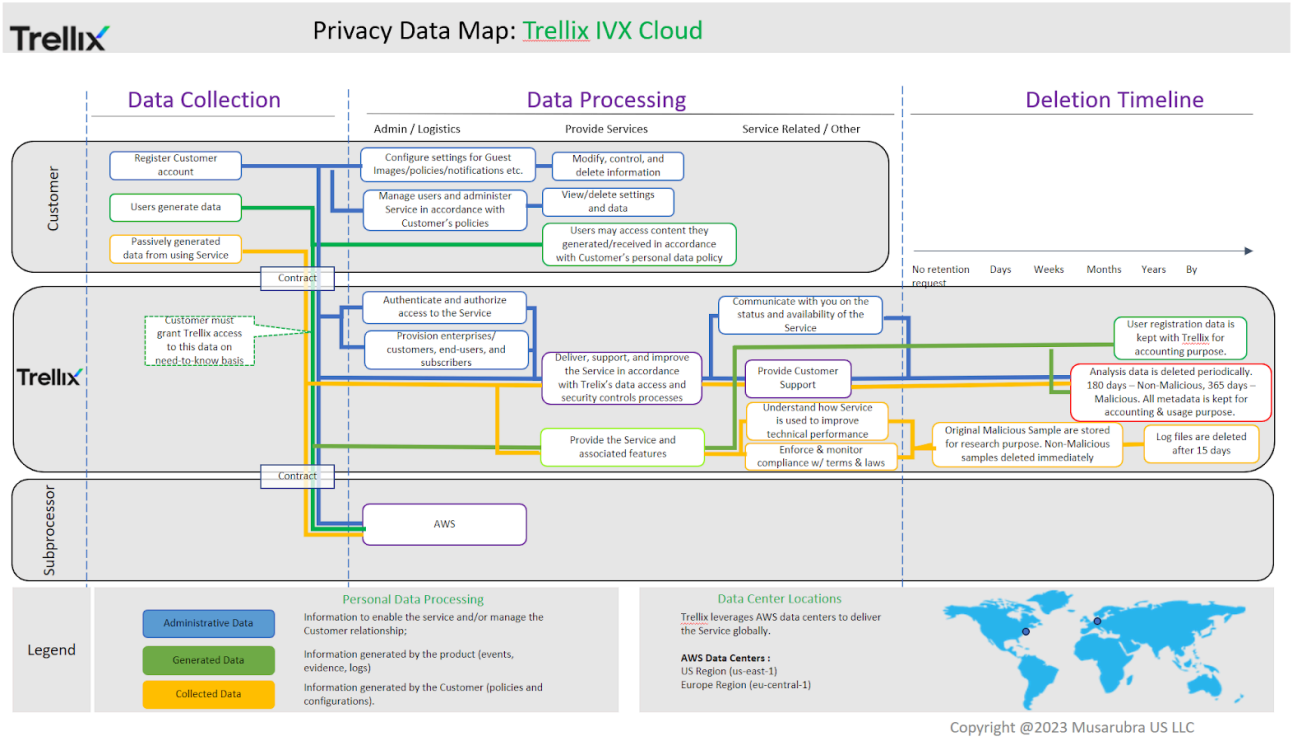
Table 4. Access Control

Personal Data Category	Who has access	Purpose of the access
Administrative Data (General identification information)	Customer Trellix Email Security – Cloud provides the capability of user access control to limit access to the data. The admin tenant of the Customer can use role-based access to grant selective access.	Analysis of systems and Customer access for compliance, audit and reporting
	Trellix Access is available to Customer Support, Engineering and DevOps under strict guardrails	Troubleshooting of Customer environment and configuration under request from the Customer
Generated Data (Events, Incidents and Evidence)	Customer Trellix Email Security – Cloud provides the capability of user access control to limit access to the data. The admin tenant of the Customer can use role-based access to grant selective access	Debugging and Troubleshooting for an alert or an incident related to email security.
	Trellix Access is available to Customer Support, Engineering and DevOps under strict guardrails	Debugging and Troubleshooting for an alert or an incident after it has been escalated by the Customer to Trellix.

Collected Data (Configuration information)	Customer Trellix Email Security – Cloud provides the capability of user access control to limit access to the data. The admin tenant of the Customer can use role-based access to grant selective access.	Analysis of systems and Customer access for compliance, audit and reporting
	Trellix Access is available to Customer Support, Engineering and DevOps under strict guardrails	Troubleshooting of Customer environment and configuration under request from the Customer

Trellix IVX - Cloud 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 IVX - Cloud 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 IVX - Cloud 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 IVX - Cloud, 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	For as long as the customer has the service	Reporting, providing the service, and troubleshooting
Generated Data	Malicious Metadata: 180 Days Non-Malicious Metadata: Only basic information of submission is kept for Customer usage tracking	Analysis and research purposes

Collected Data	Malicious Data: 365 Days Non-Malicious Data: 90 Days	Analysis and research purposes

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 IVX - Cloud 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 IVX - Cloud 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 may 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. Where Trellix is a Data Processor, users may be redirected to the Data Controller (e.g., the user's employer) or other organization for an appropriate 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.

The information provided in this document is for general awareness only, may be subject to change, and does not constitute legal or professional advice. Except as provided by the terms of a written agreement, the information and services described herein are provided “as is” with no warranty of any kind.