Trellix Privacy Data Sheet We bring security to life.

Trellix Extended Detection and Response (XDR)

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

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

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

Product Overview

Trellix XDR provides security operations teams with effective extended threat detection and response to rapidly stop attacks and keep organizations safe. Chief Information Security Officers (CISOs) and Security Operations (SecOps) teams rely on XDR for insightful visibility, simplified analysis, improved detection effectiveness, immediate automated responses, and attack mitigation.

XDR analyzes organizational-level assets (or entities) such as users and hosts to identify potential insider threats. This detects behavior anomalies by these assets, creates detections, and alerts the system immediately.

[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."

With Trellix XDR, Customer's SecOps teams can automatically identify known and unknown cyber threats with network-to-endpoint detection correlated to Trellix Global Threat Intelligence for threat analytics. XDR also combines threat event information from third-party applications to detect, enrich, explore and learn about the latest intelligence on cyber threats.

Combined with other Trellix SaaS offerings (including, for example, Trellix Global Threat Intelligence (Trellix GTI) and Trellix Endpoint Security (Trellix HX)), the Trellix XDR leverages the cloud to monitor and act on the full spectrum of new and emerging threats in real time, across all vectors—file, web, message, and network.

Trellix Customers use XDR to index, archive, search and analyze hidden patterns and anomalies in data for known and unknown cyber threats detected through alerts and event data from all sources across the Customer endpoint infrastructure. XDR allows Customers to integrate and improve security operations whether it is located on the Customer's physical premises, in the cloud, or in a hybrid environment consisting of on premise and cloud appliances and/or applications.

The Trellix XDR solution:

- Uses native and open controls to seamlessly integrate with the Customer's existing security deployment;
- Detects and prioritizes high-impact threats leveraging AI-driven security analytics, customized real-time detections, and curated contextual intelligence; and
- Streamlines threat investigations with an intuitive, guided solution built for SOC teams by security analysts.

Trellix XDR includes the following security features:

- **Cloud Connect -** XDR Cloud Connect allows events and logs from Trellix products and other third-party applications to be sent to the XDR service. Cloud Connect enables data ingestion from a variety of sources, including endpoint devices, cloud applications, and other components that comprise an enterprise network infrastructure. XDR then analyzes this data to identify potential threats and security incidents. With Cloud Connect, Trellix XDR Customers quickly and easily integrate existing applications into the XDR service without complex custom configuration.
- **Identity Access Management (IAM) -** Trellix Customer personal information is captured from client endpoints, networks, emails, attachments, or generally any entry point to an endpoint infrastructure. To administer the service, personal information about SecOps team members who directly engage with the XDR service is captured when they are granted access to the XDR interface.
- **Search Feature (Threat Hunting) -** XDR provides advanced search capabilities on ingested event data for the purpose of threat hunting, auditing, and in support of investigative activities.

- **Incident Response:** XDR allows security teams to respond to security alerts, investigate suspicious activity, and manage investigations until remediation.
- **Automated Response -** Enables security teams to integrate 3rd party tools with Helix in order to create streamlined response workflows, increasing efficiency and time to remediation.
- **Appliance Management:** XDR provides capabilities to manage and configure Trellix Endpoint, Network, and Email appliances.

XDR can be implemented as a Trellix managed deployment - Available to install by the Customer's systems administrator to configure settings through the interface.

As a result, XDR is hosted in Trellix instance in Amazon Web Services cloud infrastructure:

- Upgrades, updates and hotfixes are managed by Trellix.
- Trellix Customers access XDR via a public web portal.
- Trellix Customers configure other Trellix products to send data to the XDR service.
- Trellix Customers use the Trellix Commbroker and/or Evidence Collector to capture events occurring within their own environment.

Please also see Trellix XDR Platform for additional information related to the Trellix Extended Detection and Response (XDR) solution.

Personal Data Processing

The Trellix XDR solution uses Trellix machine learning technology to proactively and automatically monitor and detect malicious activity and policy violations occurring on the Customer's enterprise endpoints. The XDR solution provides analysis of detected threat activity and policy violations. Trellix's machine learning modules analyze event information, in online and offline modes, from the Customer's enterprise endpoints and decide how to respond based on file reputation, rules, and reputation thresholds, for both traditional and advanced file-less threats.

- **Managed deployment of XDR** - The captured event information is sent automatically via Cloud Connector by way of SSL/HTTPS connection within the Customer's network environment.
  - Note that when in transit, data is sent in clear text (no read capabilities).

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

Table 1. Personal Data Processed by Trellix Extended Detection and Response

Personal Data Category	Types of Personal Data Processed	Purpose of Processing
Administrative Data	General identification information: ● Security Operator Username ● Security Operator Email Address ● Security Operator Phone Number	Used to manage business operations ensuring compliance, provide reporting, and facilitate troubleshooting.

	● Security Operator Full Name ● Email Address Recipient ● Email Address Sender ● IP Address ● Destination IP Address ● Geolocation IP Address ● Internal IP Address ● Source IP Address ● MAC Address	
Generated Data	● Alerts ● Threats ● Correlations ● Event Data sent by the Customer into XDR	Used for threat detection and response.
Collected Data	● Event Data sent by the Customer into XDR's SIEM feature. Attributes vary by Customer based on what events they send into Helix. Common attributes found in event logs include: ○ Device or Application Name ○ Device or Application Version ○ Operating System ○ Source IP Address ○ Destination IP Address ○ Device ID (e.g. mac address) ○ Event Time	Used for Helix's SIEM feature for searching, threat hunting, and auditing.

***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

Trellix uses its own data centers as well as third-party infrastructure providers to deliver the service globally. XDR processes the personal data in AWS regional clouds located in the United States, Australia, Canada, Japan, Europe, 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 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	AWS West (Oregon)
AWS	Australia (Sydney)
AWS	Montreal
AWS	Japan (Tokyo)
AWS	Germany (Frankfurt)
AWS	Singapore

Subprocessors

Trellix partners with service providers that act as subprocessors for the XDR 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	AWS West (Oregon)
AWS	See Table 1	Hosting	Australia (Sydney)
AWS	See Table 1	Hosting	Montreal
AWS	See Table 1	Hosting	Japan (Tokyo)
AWS	See Table 1	Hosting	Germany (Frankfurt)
AWS	See Table 1	Hosting	Singapore
Pendo	Administrative Data	UI Analytics	Not Applicable
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.

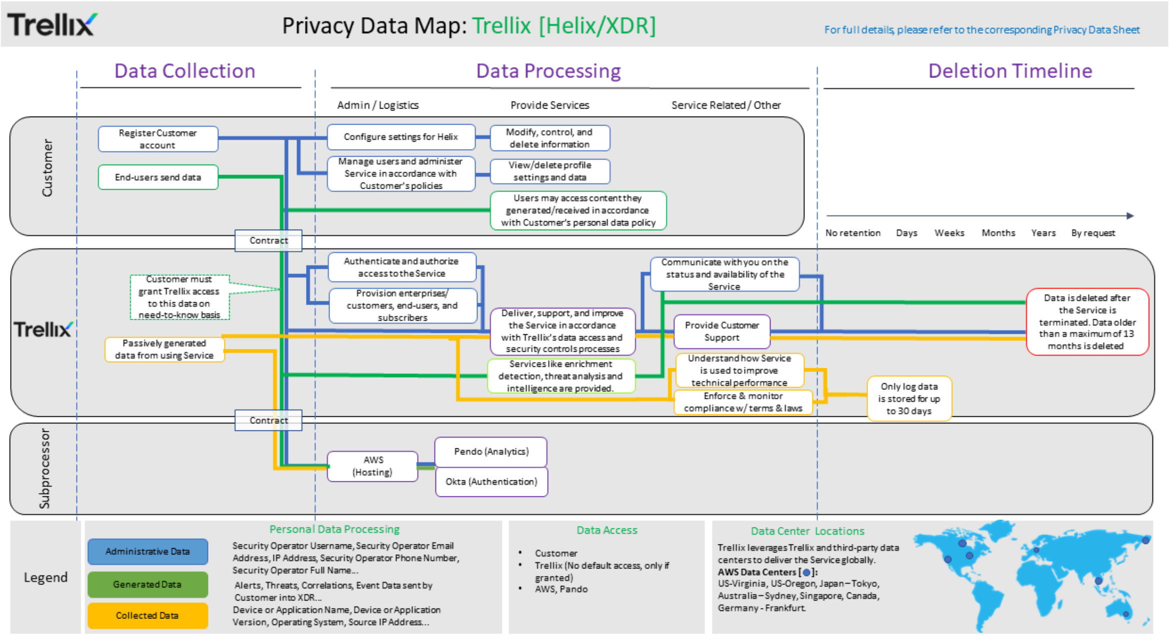
The table below lists the personal data used by XDR to carry out the service, who can access that data, and why.

Table 4. Access Control

Personal Data Category	Who has access	Purpose of the access
Administrative Data	Customer	Configuration of XDR settings and user management.
	Trellix	Provide customer support, debugging, and auditing.
Generated Data	Customer	Security monitoring, incident response.
	Trellix	Provide customer support, debugging, and auditing.
Collected Data	Customer	Security monitoring, incident response.
	Trellix	Provide customer support, debugging, and auditing.

Trellix Extended Detection and Response (XDR) Data Flow Diagram

The key data flows associated with the information processing activities described in this document are shown below.



Privacy Data Map: Trellix [Helix/XDR]

For full details, please refer to the corresponding Privacy Data Sheet

Data Collection

Data Processing

Deletion Timeline

Admin / Logistics

Provide Services

Service Related / Other

Customer

Register Customer account

End-users send data

Configure settings for Helix

Manage users and administer Service in accordance with Customer's policies

Modify, control, and delete information

View/delete profile settings and data

Users may access content they generated/received in accordance with Customer's personal data policy

No retention

Days

Weeks

Months

Years

By request

Contract

Trellix

Customer must grant Trellix access to this data on need-to-know basis

Passively generated data from using Service

Authenticate and authorize access to the Service

Provision enterprises/ customers, end-users, and subscribers

Deliver, support, and improve the Service in accordance with Trellix's data access and security controls processes

Services like enrichment detection, threat analysis and intelligence are provided.

Communicate with you on the status and availability of the Service

Provide Customer Support

Understand how Service is used to improve technical performance

Enforce & monitor compliance w/ terms & laws

Data is deleted after the Service is terminated. Data older than a maximum of 13 months is deleted

Only log data is stored for up to 30 days

Contract

Subprocessor

AWS (Hosting)

Pendo (Analytics)

Okta (Authentication)

Legend

Administrative Data

Generated Data

Collected Data

Personal Data Processing

Security Operator Username, Security Operator Email Address, IP Address, Security Operator Phone Number, Security Operator Full Name...

Alerts, Threats, Correlations, Event Data sent by Customer into XDR...

Device or Application Name, Device or Application Version, Operating System, Source IP Address...

Data Access

- Customer
- Trellix (No default access, only if granted)
- AWS, Pando

Data Center Locations

Trellix leverages Trellix and third-party data centers to deliver the Service globally.
AWS Data Centers [●]:
US-Virginia, US-Oregon, Japan – Tokyo, Australia – Sydney, Singapore, Canada, Germany - Frankfurt.

Copyright @2023 Musarubra US LLC

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 XDR 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 XDR 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., 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 XDR, 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	90 days or 13 months depending on SKU purchased.	Allows Customers to audit their users' actions.
Generated Data	90 days or 13 months depending on SKU purchased.	Allows Customers to use investigative features (e.g. search) on alert and correlation data.
Collected Data	90 days or 13 months depending on SKU purchased.	Allows Customers to use investigative features (e.g. search) on event data.

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.

Trellix XDR 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

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 XDR 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.