Trellix Privacy Data Sheet We bring security to life.

Trellix Mobile Security

The purpose of this Privacy Data Sheet is to provide Customers of Trellix Mobile Security 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 Mobile Security is a solution which protects mobile devices 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 Mobile Security subscription.

Trellix will process personal data from Mobile Security 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 Mobile Security to provide its functionality.

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

Product Overview

Trellix Mobile Security is an integrated, extensible security solution that protects iOS or Android mobile devices and enables multiple defense technologies to communicate in real time to analyze and protect against cyber threats.

Trellix Mobile Security provides active and continuous detection and mitigation of malicious events affecting devices running the iOS or Android platforms. Mobile cyber threat detection is accomplished utilizing real-time forensic data analytics provided by Trellix's enhanced machine learning detection engine. Trellix Mobile Security utilizes a central console to configure Customer designed policies and to manage threat events occurring across Trellix Customer's mobile network infrastructure.

[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."

Although Trellix Mobile Security does not require direct interaction, Trellix Customers' Security Operations Administrator (SecOps Admins) and team members (SecOps team) can interact with the Mobile Security solution to see current device security status, health, and previous events through the central management system.

Cyber threat event mitigation is performed by the Mobile Security solution and is available through Mobile Device Management (MDM) integration via a supported MDM vendor (for example, Microsoft Intune, VMware, and/or Ivanti / Mobileiron). The type of cyber threat event mitigation performed is determined by the MDM integration and can range from a simple notification to the SecOps Admin to performance of a wipe of all company data from the device.

Trellix's security experts developed a proprietary cyberattack detection engine that uses statistical models to automatically and dynamically detect advanced host and network-based attacks, as well as malicious applications on mobile devices. Unlike other threat detection systems, Trellix's Mobile Threat Detection (MTD) monitors the whole mobile device for malicious behavior without reliance on signatures. This approach allows Trellix to find and protect against both known and unknown threats in real-time, regardless of the threat source and with or without being connected to the Internet.

In addition, for Android and iOS with MDM integration, the MTD engine scans for suspicious applications installed on the device and scans applications prior to being installed to offer continuous protection. If malware is detected during scanning, action can be taken to remove a suspicious application even if the device has no network connectivity. If an internet connection is available, Trellix Mobile Security performs additional malware scanning analysis against Trellix's proprietary database.

Trellix Mobile Security consists of the following security features:

- **Always-on defense for on-the-go devices –** Unlike cloud-based mobile security solutions that rely on app sandboxing or traffic tunneling, Trellix Mobile Security sits directly on mobile devices to provide always-on protection no matter how a device is connected—corporate network, public network, cellular carrier, or even offline.
- **Advanced analysis thwarts advanced attacks –** Machine learning algorithms analyze deviations to device behavior and make determinations about indicators of compromise to accurately identify advanced device, application, and network-based attacks.
- **A single console for all devices—including mobile –** As an integrated component of Trellix Device Control, Mobile Security extends visibility and control of your mobile assets from the same single console of all your Trellix-managed devices, including operating system-based endpoints, servers, containers, and embedded Internet of Things (IoT).
- **Easy integration with 3rd party MDM providers –** Easily integrates with the most common mobile device management providers including Microsoft / Intune, VMware, Ivanti / Mobileiron, Blackberry, Jamf, Soti and Citrix.
- **PDF Scanning –** Customers can share PDFs with MTD, where they can be scanned to detect whether they are malicious or contain phishing links.
- **Zero-Touch Activation –** A new zerotouch variable allows Sec Ops Admins to configure MTD via a supported MDM vendor.
    - Note: Zero-touch activation must be set up separately, such as through a VPN profile or a supervised web content filter profile.

Trellix Mobile Security can be implemented as one of three deployments:

- **Trellix Mobile Security via Zimperium Virtual Cloud**: Customers are hosted in a Zimperium managed shared VPC or dedicated VPC utilizing Oracle, or Amazon Web Services (AWS) cloud hosted by Trellix. Zimperium also supports deployments On-Prem or to private cloud infrastructure.

- **Trellix Mobile Security via ePolicy Orchestrator On Premises (ePO On - Prem):** Customers use tenant credentials (Trellix Agent) for ePO On - Prem to view the dashboards options to track detections, activities, and status of their managed endpoint systems within their organization; or,

- **Trellix Mobile Security via ePolicy Orchestrator SaaS (ePO - SaaS):** Customers use tenant credentials (Trellix Agent) for ePO - SaaS to to view the dashboards options to track detections, activities, and status of their managed endpoint systems within their organization.

Trellix Mobile Security can be deployed through one of two integrations:

- **With Mobile Device Management (MDM) integration -** Trellix Mobile Security is pushed to an iOS or Android enterprise device from the MDM, then the device may be automatically and transparently activated without the user having to activate it manually. Device activation can be automatic and transparent to Trellix Customer's users if:
    - ➢ The vendor-specific MDM supports zero-touch activation with Trellix Mobile Security.
    - ➢ MDM integration is enabled in Mobile Console.
    - ➢ The MDM is then configured to auto-activate the device. If all conditions are not met for automatic activation, then an MDM activation link is provided. With Mobile Console, the Sec Ops Admin creates activation URLs to distribute to users. Also, non-enterprise devices can be activated by the user with an activation link.
    - Please note, for MDM deployment and installation information, follow the instructions to complete the MDM integration with the specific vendor-related MDM guide.

- **Without MDM integration -** Customers download the Trellix Mobile Security application from the Apple App Store or Google Play.

Trellix Customers' users are typically invited through an email either generated from the Mobile Console or sent by the SecOps Admin for associated devices. The SecOps Admin then provides users with required information for activation or requests that the Mobile Console send a welcome email. Once activated, the device is then matched up with the correct environment for the activation link.

Please also see Trellix Mobile Security for additional information related to the Trellix Mobile Security solution.

Personal Data Processing

Trellix Mobile Security solution uses Trellix machine learning technology and human intervention to automatically and proactively monitor and detect malicious activity and policy violations occurring on Trellix Customers' enterprise mobile devices.

Trellix's machine learning modules analyze event information, in online and offline modes, and determines how to respond based on file reputation, rules, and reputation thresholds, for both traditional and advanced file-less threats. Therefore, Trellix will capture information differently depending on the Trellix Mobile Security deployment version:

- **Trellix Mobile Security deployment via Zimperium Virtual Cloud:** The captured event information is sent via Trellix's ePO on Prem service by way of TLS version 1.2 encryption to the Customer's network infrastructure environment.
- **Trellix Mobile Security deployment via Trellix ePO On-Prem:** The solution reads data stored on the Customer's network endpoints and no data is captured by Trellix.
- **Trellix Mobile Security deployment via Trellix ePO SaaS:** The captured event information is sent automatically to Trellix Agent by way of SSL/HTTPS connection to Trellix's instance in Amazon Web Services (AWS) regional clouds.

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

Table 1. Personal Data Processed by Trellix Mobile Security

Personal Data Category	Types of Personal Data Processed	Purpose of Processing

Administrative Data	<u>General Identification Information of Sec Ops Admin:</u> ● Administrator's email address (required only for SSO/SAML.) ● First Name ● Last Name ● Phone number of the administrator (only necessary for a 2-factor authentication) <u>Device Data</u>: ● Device Login ● Device Threat Detection ● Device Periodic ● Device Location: o Street o City o Country o IP Address ● Operating System and Version ● Device Manufacturer ● Device Model ● Device Processes Running (current)	To protect mobile devices from device, application, network threats and other malicious activity. Also, for mobile threat support services.
Generated Data	<u>Network Information</u>: ● External IP Address (optional and can be disabled by the customer) ● Connection details (SSID, BSSID, External IP address): Any external service will always collect the device IP address in the system logs for investigative or forensic purposes), Gateway IP and MAC, List of names of all nearby WLAN networks visible to the mobile device, ARP and routing table, Mobile carrier + country code, Attacker IP and MAC address, Risky and other unwanted URLs e.g., phishing and blocked web categories) ● Gateway IP Address ● Gateway MAC Address	To protect mobile devices from device, application, network threats and other malicious activity. Also, for mobile threat support services.

	● Nearby Wi-Fi networks: Android shows the network name (SSID) and BSSID of the nearby Wi-Fi networks
	● ARP Table
	● Route Table
	● Carrier Information:
	  ○ Attacker network details
	  ○ IP Address
	  ○ MAC Address	

Collected Data	App Data Detection Information: ● Application Forensics: This forensics information is shown, if requested. (Optional) ● Application Binaries ● Application Inventory ● App metadata like app name, bundle-ID, hash, developer certificate information (optional and can be disabled by the customer) ● Android app copy (optional and can be disabled by customer) ● Android app inventory list (optional and can be disabled by customer) ● iOS profiles (name, category (e.g., WebClip or CA), description, status (e.g., managed/not managed) ● Apps (app name + version, bundle ID/package name; hash; status (e.g., managed/not managed), platform iOS/Android)	To protect mobile devices from device, application, network threats and other malicious activity. Also, for mobile threat support services.

***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 Zimperum for Trellix ePO - On Prem deployment, the data center is located within the Customer's network infrastructure.

For Zimperium Virtual Cloud deployment, Zimperium processes the personal data in OEM Zimperium's instances in AWS regional clouds located in the United States, Germany, Australia, Tokyo and Singapore. Zimperium's regional clouds provide options to address customers' data location preference where Customers have the choice to select a region or to default to their nearest region for data processing.

Table 2a. Data Center Locations - Zimperium for Trellix ePO - SaaS

Data Center Provider	Data Center Location
AWS	AWS West (Oregon)
AWS	AWS East (Virginia)
AWS	Germany (Frankfurt)
AWS	Australia (Sydney)
AWS	Japan (Tokyo)
AWS	Singapore
AWS	Additional AWS locations upon request

For Trellix ePO - On Prem deployment, the data center is located within the Customer's network infrastructure.

For Trellix ePO - SaaS deployment, Trellix uses its own data centers as well as third-party infrastructure providers to deliver the service globally. ePO - SaaS processes the personal data in Trellix's instance in Amazon Web Services, Inc. (AWS) regional clouds located in the United States, Germany, Australia, Singapore, and India. 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 2b. Data Center Locations - Trellix ePO - SaaS

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

Subprocessors

Trellix partners with service providers that act as subprocessors for the Mobile Security 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 - Trellix ePO - SaaS

Subprocessor	Personal Data Category	Service Type	Location of Data Center
Zimperium	See Table 1	Mobile Threat Detection	See Table 2a.
AWS	See Table 1	Data Center	Germany (Frankfurt)
AWS	See Table 1	Data Center	Australia (Sydney)
AWS	See Table 1	Data Center	Singapore
AWS	See Table 1	Data Center	India (Mumbai)
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 function. 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 Mobile Security to carry out the service, who can access that data, and why.

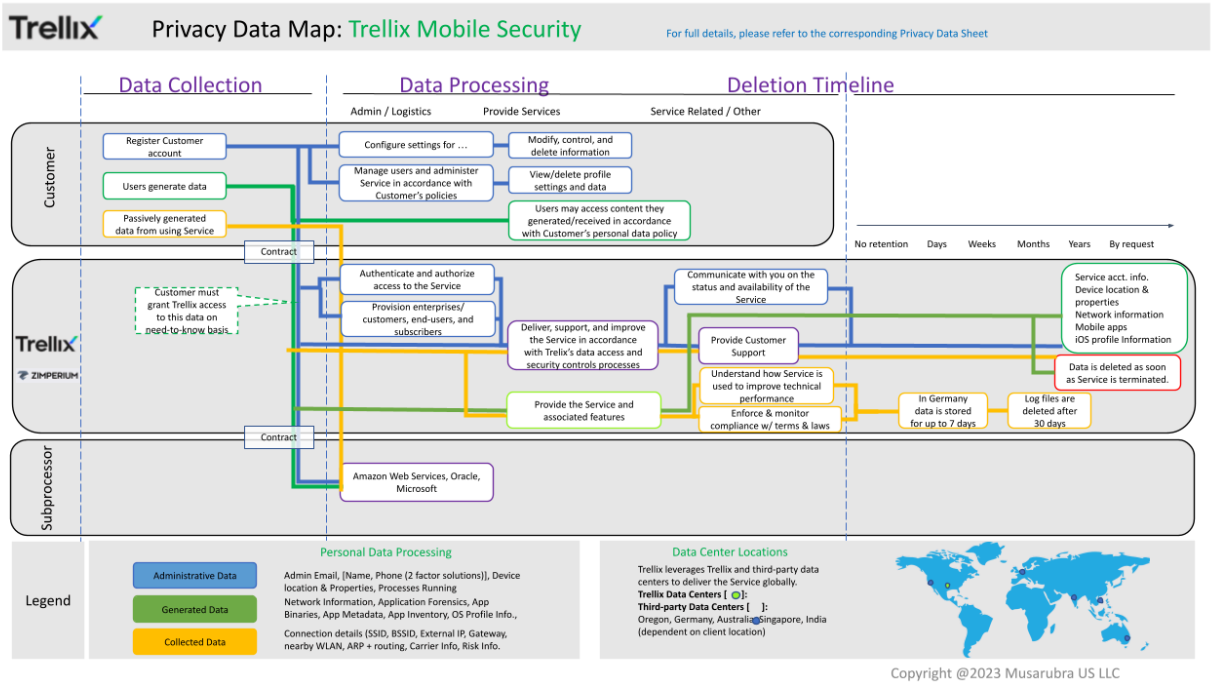
Table 4. Access Control

Personal Data Category	Who has access	Purpose of the access

Administrative Data	Customer	Administration of tools for protection of mobile devices from device, application, network threats and malicious activity.
	Trellix	Customer Support.
Generated Data	Customer	Protection of mobile devices from device, application, network threats and other malicious activity. Also, to provide support in relation to the mobile threat defense services.
	Trellix	Protection of mobile devices from device, application, network threats and other malicious activity. Also, to provide support in relation to the mobile threat defense services.
Collected Data	Customer	Protection of mobile devices from device, application, network threats and other malicious activity. Also, to provide support in relation to the mobile threat defense services.
	Trellix	Protection of mobile devices from device, application, network threats and other malicious activity. Also, to provide support in relation to the mobile threat defense services.

Trellix Mobile 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 Mobile Security 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 Mobile Security 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 Mobile Security, 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	Duration of the provision of services under the Agreement.	Required for systems operation and reporting to Customer.
Generated Data	Duration of the provision of services under the Agreement.	Required for systems operation and reporting to Customer.
Collected Data	Duration of the provision of services under the Agreement.	Required for systems operation and reporting to Customer.

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 Mobile Security 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 Mobile Security 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.