

# Cloud Workload Protection Platform

## CWPP Policy

### Product Documentation



## Copyright Notice

©2013-2023 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

## Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

## Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

# Contents

CWPP Policy

Data Processing And Security Agreement

# CWPP Policy

## Data Processing And Security Agreement

Last updated : 2023-12-26 16:41:21

### 1. BACKGROUND

This Module applies if you use Cloud Workload Protection Platform (CWPP) (“**Feature**”). This Module is incorporated into the Data Processing and Security Agreement located at (“**DPSA**”). Terms used but not defined in this Module shall have the meaning given to them in the DPSA. In the event of any conflict between the DPSA and this Module, this Module shall apply to the extent of the inconsistency.

### 2. PROCESSING

We will process the following data in connection with the Feature:

Personal Information	Use
<p>Client Protected Resource Information:</p> <p><b>For protection of Tencent Cloud servers:</b> APPID, UIN, your servers information (name, IP address, type, OS, agent version, agent installment date, time of last login, online status, installed components, and security level)</p> <p><b>For protection of non-Tencent Cloud servers:</b> resource monitoring, account, port, software application, process, database, web application, web service, web framework, web site, jar package, startup service, scheduled task, environment variables, kernel module</p>	<p>We only process this data for the purposes of providing the Feature to you. Please note that unless authorized by you, we have no access to the personal data, if any, stored in the database or control over the data.</p> <p>Please note that this data is stored and backed up in our TencentDB for MySQL (MySQL) feature.</p>
<p>Security Incident Information:</p> <p><b>For the free subscription of the Feature:</b></p> <p>Intrusion detection information: events such as client server abnormal login, password cracking; information regarding the relevant events (server UUID, event details, threat level, and processing status).</p> <p><b>For the paid subscription of the Feature, the following are additionally processed:</b></p> <p>Detection information on servers' security holes: UUID of affected servers, name and descriptions of detected security holes, current status, date and time of the latest detection;</p>	<p>We only process this data for the purposes of providing the Feature to you. We may also anonymize and de-identify certain security incident information to improve the Feature.</p> <p>Please note that this data is stored and backed up in our MySQL feature.</p>

<p>Security baseline information: UUID of servers, name of security baseline, detection type, security threat levels, current status, date and time of the latest detection;</p> <p>Security report of the servers: total number of logged client abnormal login, vulnerability scanning results, password cracking, and malicious file scanning; numbers and types of purchased subscriptions of the Feature by you.</p>	
<p>Client Configuration Data:</p> <p>Detection configuration of vulnerabilities/baselines/files: regular detection settings, ignored vulnerabilities/baselines, trusted files, quarantined files;</p> <p>Whitelist configuration of intrusion prevention functions: whitelist conditions, covered servers;</p> <p>Other configurations: automatic protection upgrade settings, automatic renewal settings, and alarm settings.</p>	<p>We only process this data for the purposes of providing the Feature to you in accordance to your specific configuration.</p> <p>Please note that this data is stored and backed up in our MySQL feature.</p>

### 3. SERVICE REGION

As specified in the DPSA.

### 4. SUB-PROCESSORS

As specified in the DPSA.

### 5. DATA RETENTION

We will store personal data processed in connection with the Feature as follows:

Personal Information	Retention Policy
<p>Client Protected Resource Information Security Incident Information Client Configuration Data</p>	<p>We retain such data until you manually delete such data. Otherwise, when you terminate your subscription for the Feature or delete your account, we will delete such data within 7 days.</p>

You can request deletion of such personal data in accordance with the DPSA.

### 6. SPECIAL CONDITIONS

You must ensure that this Feature is only used by end users who are of at least the minimum age at which an individual can consent to the processing of their personal data. This may be different depending on the jurisdiction in which an end user is located.