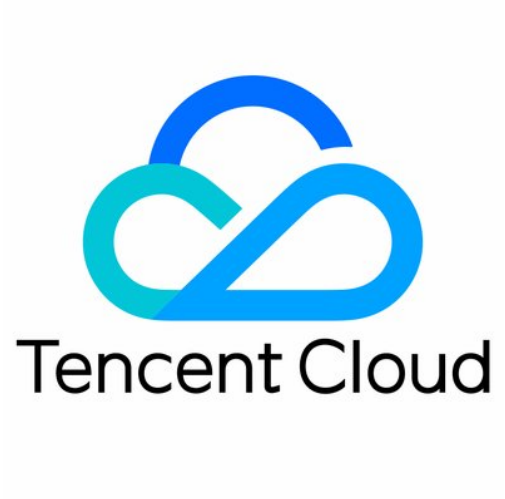
Vulnerability Scan Service

VSS Policy

Product Documentation



Contents

VSS Policy
Privacy Policy

Last updated：2022-02-28 14:43:57

1. INTRODUCTION

This Module applies if you use Vulnerability Scan Service ("**Feature**"). This Module is incorporated into the privacy policy located at Privacy Policy. Terms used but not defined in this Module shall have the meaning given to them in the Privacy Policy. In the event of any conflict between the Privacy Policy and this Module, this Module shall apply to the extent of the inconsistency.

2. CONTROLLERSHIP

The controller of the personal information described in this Module is as specified in the Privacy Policy.

3. AVAILABILITY

This Feature is available to users globally but primarily intended for users located in the same country/region as the selected service region for optimal performance.

4. HOW WE USE PERSONAL INFORMATION

We will use the information in the following ways and in accordance with the following legal basis:

Personal Information	Use	Legal Basis
Vulnerability Scanning Engine Operating Data: engine operation time, engine operation count, engine operation status, engine task log data	We use this information to ensure the engine functions as required, to provide this Feature to you. Please note that this data is stored in our TencentDB for Redis (Redis), TencentDB for MySQL (MySQL) and TencentDB for MongoDB (MongoDB) features for this purpose.	We process this information as it is necessary for us to perform our contract with you to provide the Feature.
Asset Mapping Engine Operating Data: map of engine operation	We use this information to provide this Feature to you, including to generate security scan, risk and related	We process this information as it is necessary for us to

	reports, provide risk warnings and vulnerability detection notifications, and provide repair suggestions. Please note that this data is stored in our Redis, MySQL and MongoDB features for this purpose.	perform our contract with you to provide the Feature.
User Quota Data: expiry date and time, number of domain names, number of IPs, number of APIs	We use this information to calculate your user quota and charge, for billing purposes. Please note that this data is stored in our Redis, MySQL and MongoDB features for this purpose.	We process this information as it is necessary for us to perform our contract with you to provide the Feature.
Task Log Data: task name, monitoring type, scanned asset scanning plan, scanning speed, scanning duration, scanning result	We use this information to provide this Feature to you, and for troubleshooting. Please note that this data is stored in our TencentDB for Redis, TencentDB for MySQL and TencentDB for MongoDB features for this purpose.	We process this information as it is necessary for us to perform our contract with you to provide the Feature.
Vulnerability Matching Data: Vulnerability name, threat level, affected assets, vulnerability type, time when last found	We use this information to provide this Feature to you, and for troubleshooting. Please note that this data is stored in our TencentDB for Redis, TencentDB for MySQL and TencentDB for MongoDB features for this purpose.	We process this information as it is necessary for us to perform our contract with you to provide the Feature.
Port Matching Data: port, vulnerability response suggestions, protocol, port service	We use this information to provide this Feature to you, and for troubleshooting. Please note that this data is stored in our TencentDB for Redis, TencentDB for MySQL and TencentDB for MongoDB features for this purpose.	We process this information as it is necessary for us to perform our contract with you to provide the Feature.

5. HOW WE SHARE AND STORE PERSONAL INFORMATION

As specified in the Privacy Policy.

6. DATA RETENTION

We will retain personal information in accordance with the following:

Personal Information	Retention Policy

Vulnerability Scanning Engine Operating Data	Stored for 7 days.
Asset Mapping Engine Operating Data	Stored for 7 days.
User Quota Data	We retain such data for as long as you use the Feature. When your use of the Feature is terminated, we will delete this data after 7 days.
Task Log Data	We retain such data for as long as you use the Feature. When your use of the Feature is terminated, we will delete this data after 7 days.
Vulnerability Matching Data	We retain such data for as long as you use the Feature. When your use of the Feature is terminated, we will delete this data after 7 days.
Port Matching Data	We retain such data for as long as you use the Feature. When your use of the Feature is terminated, we will delete this data after 7 days.

Data Processing And Security Agreement

Last updated：2022-02-28 15:06:59

1. BACKGROUND

This Module applies if you use Vulnerability Scan Service ("**Feature**"). This Module is incorporated into the Data Privacy 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
Basic Website Information: Asset address, type, additional time (if more resources are required after the vulnerability scan), authentication status, mock login status, last scan time	We only process this data for the purposes of providing this Feature to you. Upon your request, we will also process this data for troubleshooting. Please note that this data is stored in our TencentDB for Redis, TencentDB for MySQL and TencentDB for MongoDB features for this purpose.
Basic Host Information: Server IP, additional time (if more resources are required after the vulnerability scan), authentication status, last scan time	We only process this data for the purposes of providing this Feature to you. Upon your request, we will also process this data for troubleshooting. Please note that this data is stored in our TencentDB for Redis, TencentDB for MySQL and TencentDB for MongoDB features for this purpose.
Basic API information: API name, API domain name, authentication method, authentication status, additional time (if more resources are required after the vulnerability scan), result of last scan, time of last scan	We only process this data for the purposes of providing this Feature to you. Upon your request, we will also process this data for troubleshooting. Please note that this data is stored in our TencentDB for Redis, TencentDB for MySQL and TencentDB for MongoDB features for this purpose.
Task Configuration Data: task name, type, monitored asset, scanning plan, scanning period, scanning speed, last scan, status	We only process this data for the purposes of providing the Feature to you in accordance to your specific configuration. Please note that this data is stored in our TencentDB for Redis, TencentDB for MySQL and TencentDB for MongoDB features

	for this purpose.

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**
Basic Website Information	We retain such data for as long as you use the Feature. You may manually delete such data on the Feature. Once you choose to delete such data or terminate your use of the Feature, we will delete this data after 7 days.
Basic Host Information	We retain such data for as long as you use the Feature. You may manually delete such data on the Feature. Once you choose to delete such data or terminate your use of the Feature, we will delete this data after 7 days.
Basic API information	We retain such data for as long as you use the Feature. You may manually delete such data on the Feature. Once you choose to delete such data or terminate your use of the Feature, we will delete this data after 7 days.
Task Configuration Data	We retain such data for as long as you use the Feature. You may manually delete such data on the Feature. Once you choose to delete such data or terminate your use of the Feature, we will delete this data after 7 days.

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.