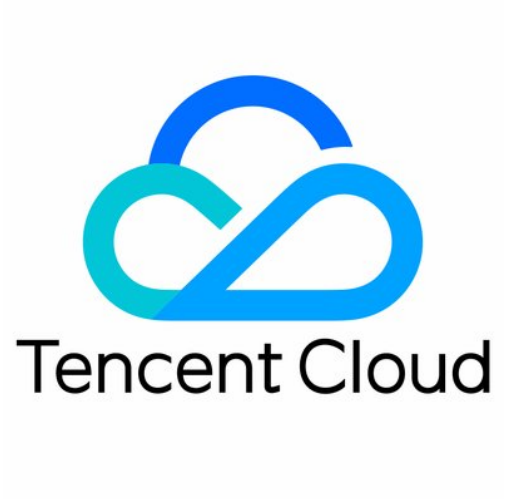
Tencent Container Security Service

TCSS Policy

Product Documentation



Contents

TCSS Policy
Privacy Policy

Last updated：2023-04-03 14:53:15

1. INTRODUCTION

This Module applies if you use Tencent Container Security 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, except Russia.

Please note that this Feature is only available if you are subscribed to our Tencent Cloud hosting services, including Cloud Virtual Machine (CVM), Edge Computing Machine (ECM),Tencent Cloud Lighthouse, and/or Blackrock Physical Server (collectively or individually (as applicable) the "**Hosting Service**").

4. HOW WE USE PERSONAL INFORMATION

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

Personal Information	Use	Legal Basis

Personal Information	Use	Legal Basis
Asset Management Data: APPID, UIN, and basic server information under your account, including: • Server basic information: server name, intranet/extranet IP, server type, operating system, client version, client installation time, last login time, online status, installed components, security protection level, instance ID, project, label, kernel version; • Container's basic information: container name/ID, running status, running user, associated image/image ID, POD, CPU usage, memory usage, host IP, process, port, data mount, network, components, running applications, web services; • Local image basic information: image name/ID, creation time, image size, operating system, number of associated hosts (including host name, host IP, host status, business group, Docker version, Docker file system type), number of associated containers (including container name, container ID, running status, CMD, last update time), image security risks (including security vulnerabilities, which includes security vulnerabilities, Trojans, sensitive information (privileged mode startup, code leakage, authentication information leakage)), build history, component information; • image warehouse basic information: image warehouse address, warehouse type, image name, image ID, image version, image size, security risks (including security vulnerabilities, Trojan horses, sensitive information (privileged mode startup, code leakage, authentication information leakage)), build history • Cluster basic information: cluster ID / name, running status of components, cluster status, cluster type, region, Kubernetes version, the total number of nodes associated with the cluster, cluster check time, cluster check status, the number of serious risks / high risks / medium risks / low risks, check mode, cluster risk (vulnerability, configuration risk)	We use this information for the purposes of providing the Feature to you, including to locate and solve container-related problems. Please note that this data is stored and backed up in our TencentDB for MongoDB (MongoDB) and TencentDB for MySQL (MySQL) features, temporarily stored and backed up in our Cloud Object Storage (COS) feature, and integrated with the relevant Hosting Service you are subscribed to.	We process this information as it is necessary for us to perform our contract with you to provide the Feature.

Personal Information	Use	Legal Basis
Container Security Data: • **Security vulnerability information:** vulnerability detection information of customer assets (affected image, cloud host where the image is located, vulnerability name, vulnerability description, processing status, and recent detection time); • **Security baseline information:** baseline detection information of your assets (containers, images, cloud hosts, clusters, baseline name, detection type, threat level, processing status, recent detection time); • **Cluster security information:** configuration of customer clusters, and vulnerability detection information (cluster, cluster type, region, risk check items, threat level, recent detection time); • **Intrusion detection information:** event status of container escape, reverse shell, file check, abnormal process, file tampering, high-risk system calls, virus scanning, malicious outgoing requests, abnormal K8s API requests, (container name/ID, event details, threat level, processing information and status, risk description, solution, hit rules, exception request log)	We use this information for the purposes of providing the Feature to you, including to locate and solve container-related problems. Please note that this data is stored and backed up in our MongoDB and MySQL features, temporarily stored and backed up in our COS feature, and integrated with the relevant Hosting Service you are subscribed to.	We process this information as it is necessary for us to perform our contract with you to provide the Feature.
Business Operation Data: security reports of customer servers (total number of risks of container escape, asset management, image risk, cluster security, baseline management, virus scanning, malicious outgoing requests, abnormal process, abnormal K8s API request, reverse shell, file check, abnormal process, file tampering, high-risk system calls; the amount of resources needed to run the container (Container Security Pro), the number of image licenses, and the amount of log analysis storage you have purchased)	We use this information for the purpose of providing the Feature to you, including providing you a security report of the Feature. Please note that this data is stored and backed up in our MongoDB and MySQL features, temporarily stored and backed up in our COS feature, and integrated with the relevant Hosting Service you are subscribed to.	We process this information as it is necessary for us to perform our contract with you to provide the Feature.

Personal Information	Use	Legal Basis
Product Configuration Data: • **Knowledge base management information:** service-side configuration information of the rules for components and vulnerabilities to be detected in the image (component name, official link, component description, component type, operator/update time, detection switch; vulnerability name/CVE, affected component, threat level, vulnerability classification, vulnerability description, repair plan, operator/update time, detection switch); • **DNS knowledge base information:** service-side configuration information of the malicious request function, malicious domain name determination rules (DNS domain name, reference links, description, open status); • **Automatic Trojan horse quarantine information:** service-side rules for the determination of Trojan horse files (MD5 blacklist, virus name blacklist, global quarantine directory, global ignore directory)	We use this information for the purposes of providing the Feature to you, and ensuring the Feature functions as required. Please note that this data is stored and backed up in our MongoDB and MySQL features, and integrated with the relevant Hosting Service you are subscribed to.	We process this information as it is necessary for us to perform our contract with you to provide the Feature.
Version Management Data (the current released versions of the installation package, based on the version selected by you when purchasing the Feature)	We use this information for the purpose of ensuring the Feature functions as required. Please note that this data is stored and backed up in our MongoDB and MySQL features, and integrated with the relevant Hosting Service you are subscribed to.	We process this information as it is necessary for us to perform our contract with you to provide the Feature.

5. HOW WE STORE AND SHARE 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
Asset Management DataContainer Security InformationBusiness Operation Data	We retain such data for a minimum of 180 days. We retain such data until you terminate your use of the relevant Hosting Service(s), in which case we will temporarily retain this data in our COS feature and delete the same (i) 30 days thereafter or (ii) after the minimum number of days required to meet the 180-days minimum data retention threshold (as applicable).
Product Configuration DataVersion Management Data	We retain such data for 180 days.

Data Processing And Security Agreement

Last updated：2023-04-03 14:53:02

1. BACKGROUND

This Module applies if you use Tencent Container Security Service ("**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
Asset Basic Data: Basic information of your servers, containers, images and clusters (asset fingerprint information (resource monitoring, accounts, ports, software applications, processes, databases, web applications, web services, web frameworks, web sites, Jar packages startup services, scheduled tasks, environment variables, kernel modules), basic information of image repository (image repository address, repository type, image name, image ID, image version, image size, security risks (including security vulnerabilities, Trojan viruses, sensitive information), construction history)	We only process this data for the purposes of providing the Feature to you. Please note that this data is stored and backed up in our TencentDB for MongoDB (MongoDB) and TencentDB for MySQL (MySQL) features, temporarily stored and backed up in our Cloud Object Storage (COS) feature, and integrated with the relevant Hosting Service (as defined in the Privacy Policy module for this Feature) you are subscribed to. If you have purchased our Tencent Kubernetes Engine (TKE) cluster, basic information of image repository is also shared with us upon your authorization, for the purpose of providing the Feature to you (including to conduct security checks).

Personal Information	Use
Console Configuration Data: • Configuration of image, cluster, vulnerability, baseline, file, log detection: regular detection, ignore vulnerability / baseline, your confirmation to trust file or isolate file, intercept process, intercept image, intercept container network access) • Whitelist configuration for container escape, reverse shell, file check, abnormal process, file tampering, high-risk system drop call and other intrusion prevention features: whitelist conditions, effective mirror rangeOther configuration information: automatic server upgrade protection settings, automatic renewal settings, alarm settings	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 and backed up in our TencentDB for MongoDB (MongoDB) and TencentDB for MySQL (MySQL) features, and integrated with the relevant Hosting Service (as defined in the Privacy Policy module for this Feature) you are subscribed to.

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
Asset Basic Data	We retain such data for a minimum of 180 days. We retain such data until you terminate your use of the relevant Hosting Service(s), in which case we will temporarily retain this data in our COS feature and delete the same (i) 30 days thereafter or (ii) after the minimum number of days required to meet the 180-days minimum data retention threshold (as applicable).
Console Configuration Data	Stored until you request for deletion, upon which such data will be deleted within 30 working days. Where you do not request for deletion, such data will be deleted after 1 month of termination of your use of this Feature, unless otherwise required by applicable data protection laws.

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.

This Feature is not intended for the processing of sensitive data. You must ensure that this Feature is not used to transfer or otherwise process any sensitive data by you or your end users.