Cloud Security Center

Purchase Guide

Copyright Notice

Trademark Notice

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

Purchase Guide
Cloud Security Center (New Version)
Billing Overview

Last updated：2023-09-01 14:20:17

Release notes

Tencent Cloud Security Center offers three paid versions: Advanced, Enterprise, and Ultimate. Each version is differentiated by its features and default specifications to cater to customers of varying scales and needs. The specifications details are as follows:

Billing		Free Edition	Premium Edition	Enterprise Edition	Ultimate Edition	Elastic Expansion
Base Price		-	CNY 1800/month	CNY 4800/month	CNY 12800/month	-
Available Purchase Duration		-	3 months, 6 months, 1 year, 2 years, 3 years	1 month, 3 months, 6 months, 1 year, 2 years, 3 years		-
Discount		-	Purchases of 6 months or less: No discount 1-year purchase: 15% off Purchase for 2 years: 30% off Purchase for 3 years: 50% off			-
Asset and risk management	Comprehensive solution	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	-
	Asset Center	This feature is	This feature is supported.	This feature is	This feature is supported.	-

	supported.		supported.		
Asset health scan times	20 times/month	400 times/month	1,200 times/month	4,800 times/month	CNY 1200/300 times/month
Scan Task Management	1	10	20	50 (can be set as unlimited)	-
Port Risks Scan	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	-
Emergency vulnerability scan	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	-
In-depth vulnerability scan	-	This feature is supported.	This feature is supported.	This feature is supported.	-
Weak password scan	-	This feature is supported.	This feature is supported.	This feature is supported.	-
Cloud resource configurations scan	-	This feature is supported.	This feature is supported.	This feature is supported.	-
Content Scanni	-	-	This feature is	This feature is	-

	ng (Website Content Risk)			supported.	supported.	
Attack and alarm handling	Log analysis	–	1,000 GB/month	3,000 GB/month	10,000 GB/month	CNY 500/1,000GB/month
	Alarm connection	This feature is supported.	This feature is supported.	This feature is supported.	This feature is supported.	–
	Alarm aggregation, event investigation, and relational analysis	–	This feature is supported.	This feature is supported.	This feature is supported.	–
	Joint Handling	–	–	This feature is supported.	This feature is supported.	–
management	Security report	–	Medical report	Inspection interpretations	Expert insights	–
	Log shipping (Shipping to	–	–	–	This feature is supported.	–

	Ckafka)					
	Multiple account management	-	-	-	Scalable	CNY 3,000/account/month, no additional charges for more than 10 accounts. If a member account has purchased the Ultimate Edition, the multi-account feature is free.

Selection Guide

Cloud Security Center is a one-stop cloud security management platform that offers three packages: Advanced, Enterprise, and Ultimate, depend on different user needs. We recommend you choose the package that best suits your needs based on the number of cloud assets, group accounts, log audits, and security assurance during critical periods:

Feature	Premium Edition	Enterprise Edition	Ultimate
The number of cloud assets, such as: public IP, domain name, host, load balancing, database, COS object storage, Elasticsearch Service, etc.	100	300	900 and above
whether to use Tencent Cloud's organization account solution.	Not required	Not required	Supported
is there a need for unified integration of security product logs for analysis and management.	Not required	Supported	Supported

Is there a need for internet attack and defense drills during critical periods?	Not required	Supported	Supported

Asset Check Notes

- Cloud Security Center supports security health checks for assets, covering aspects such as ports, weak passwords, emergency vulnerabilities, In-depth vulnerabilities, service exposure, website content risks, and cloud resource configurations.
- Each scan consumes an Asset health scan times, which means, scanning one asset (for example: public IP, domain, host, load balancing, database, COS object storage, ElasticsearchService, etc.) consumes one asset scan times. The Advanced, Enterprise, and Ultimate editions of Cloud Security Center include 400, 1200, and 4800 asset scan times respectively, and support paid expansion.
- To mitigate asset security risks, it is recommended to conduct four automatic checks and one comprehensive manual check each month. Please calculate the number of asset health checks to purchase based on the quantity of your cloud assets.

Billing Modes

Last updated：2023-09-01 14:20:43

1. Navigate to the Cloud Security Center purchase page , select a package according to your needs, or set the purchase content as per your requirements. The system will automatically calculate the necessary costs for you.
2. Once your selection is complete, click **Place Order Now**. Completing the payment process will successfully finalize your purchase.

Renewal Policy

Last updated：2023-09-01 14:20:54

Resources in the Cloud Security Center will be destroyed 14 days after expiration (for details, please refer to Cloud Security Center - Overdue Payment Instructions). To ensure the stable and normal operation of the service, you need to pay attention to the expiration time of the Cloud Security Center package and remember to renew it before it expires. It is recommended that you set the Cloud Security Center to auto-renew upon expiration. You can also manually renew resources on the Cloud Security Center Renewal Page or in the Billing Center.

Overdue Policy

Last updated：2023-09-01 14:21:05

- On the day of product expiration, the Cloud Security Center package will be adjusted to the free version.
- The product features and specifications will be adjusted to the free package, and paid features such as deep vulnerability scanning, weak password scanning, and cloud resource configuration checks will become unavailable.
- Fourteen days after the product expiration, the system will reclaim all resources of the Cloud Security Center, delete the configuration information which cannot be restored, and it can only be reconfigured after repurchasing.

Gift instructions

Last updated: 2023-09-01 14:31:03

Event Duration

From April 30, 2023, 00:00:01 to December 31, 2023, 23:59:59.

Participants

All domestic users who have registered and completed identity verification on the Tencent Cloud official website are eligible to participate.

Event Overview

During the event, upon successful purchase of the Cloud Security Center product, Tencent Cloud will gift the Security Operation Center product according to the following rules:

Product Acquisition	Gifted Product
Cloud Security Center (Ultimate Edition)	Security Operations Center Premium Edition (1500 Asset Count)
Cloud Security Center (Enterprise Edition)	Security Operation Center Premium Edition (700 Asset Count)
Cloud Security Center (Premium Edition)	Security Operation Center Premium Edition (300 Asset Count)
Log analysis	Log Storage (Gifted on a 1:1 ratio according to Log Analysis volume)

Event Guidelines

- Upon purchasing a Cloud Security Center product, if users upgrade their package configuration (i.e., purchase a higher version of the Cloud Security Center product) during the event period, they will be granted additional usage specifications for the Security Operations Center product, supplementing the specifications of the Security Operations Center product that were initially gifted with the purchased version of the Cloud Security Center, up to the specifications corresponding to the upgraded version of the Cloud Security Center product.

  Example: After purchasing Cloud Security Center (Enterprise Edition) and receiving Security Operation Center Premium (700 asset count) as a gift, if the user upgrades to

Cloud Security Center (Ultimate Edition) during the event period, they are eligible to receive Security Operation Center Premium (1500 asset count) as per the event rules. Therefore, Tencent Cloud will supplement the already gifted Security Operation Center product specifications with an additional 800 asset authorizations for the Security Operation Center Premium.

- Users who have already purchased the Security Operation Center product will, upon purchasing the Cloud Security Center product, have their existing package expanded to include additional specifications of the Security Operation Center product (i.e., the specifications of the gifted product will be added to the existing package). Users who have not purchased the Security Operation Center product will, upon purchasing the Cloud Security Center product, have direct access to the Security Operation Center product and can use it via its console.

- The validity period of the complimentary product aligns with that of the purchased product. Please note that the complimentary Security Operation Center capabilities will expire simultaneously when the Cloud Security Center product expires or is refunded.

Refund

Last updated：2023-09-01 14:21:24

If you have not utilized the Cloud Security Center product, it supports a five-day unconditional return and refund within five days of purchase.
Utilizing the Cloud Security Center product refers to the use of its features, including but not limited to asset health checks. The following examples are considered as product usage and do not fall within the scope of the five-day unconditional refund:

- After purchasing the Cloud Security Center product, an asset health check task has been conducted.
- After purchasing the Cloud Security Center product, features such as simulated attacks have been utilized.
- After purchasing the Cloud Security Center product, a security health check report has been downloaded.

Refund Method

Cash vouchers purchased with cash and coupons (vouchers/discount coupons) used at the time of product purchase are non-refundable. The non-coupon costs used when purchasing the product will be refunded to the payer's Tencent Cloud account according to the payment method (cash/gift credit/cash voucher) and payment ratio.

Refund Method

Once you have confirmed compliance with the five-day unconditional refund policy, you may submit a ticket to apply for a return and refund.

Cloud Security Expert Technical Support

Last updated：2023-09-01 14:21:34

Cloud Security Expert Technical Support is a service based on the three lines of defense in cloud security (Cloud Firewall, Web Application Firewall, Workload Protection, and Container Security). It offers pre-incident security expert risk inspections and penetration testing, mid-incident monitoring of attacker behavior and standby response, and post-incident summary and review services. Cloud Security Expert Technical Support is suitable for scenarios such as security assurance during critical periods and network security attack and defense drills. It enhances an enterprise's ability to observe and intervene in its own security risks, ensuring business stability and security.

Service Content

Cloud Security Inspection Service

Provides users with risk inspections prior to network security attack and defense drills and security assurance during critical periods. It offers an overall security assessment, identifies potential security risks, and security experts provide a security inspection report along with repair suggestions.

Feature Name	Service Content	Deliverables
Shadow Asset Inventory	Inventory and streamline business assets on the cloud, streamline public IP, domain names, and other off-cloud assets. It covers six major types of assets including hosts, containers, public IPs, domain names, networks, and databases, encompassing over 30 types of assets, and provides a shadow asset inventory list.	Security Inspection Report
Internet Exposure Surface Scanning	Identifies cloud server service ports exposed to the internet, service ports exposed through CLB, service ports exposed through NAT, and various cloud resources providing open services to the internet, providing a list and repair suggestions.	
Weak password scan	Conducts weak password detection for host assets, public IP addresses, and domain Web services. It identifies improper weak password configurations for public network	

	services such as ftp, redis, etc., and provides a list along with repair suggestions.	
Cloud Resource Configuration Risk Scanning	Provides security configuration checks for relevant cloud products on Tencent Cloud, including checks on four major dimensions: computing and application configuration security, network configuration security, storage and data security, and identity access security. A checklist and repair suggestions are also provided.	
Network Security Evaluation	Assess the protection status of public network IPs and domain names, as well as the status of open ports, and provide evaluation results and repair suggestions.	
Host Security Evaluation	Inventory cloud host assets, assess host protection status and open port conditions, and provide evaluation results and repair suggestions.	
Vulnerability Risk Assessment	Comprehensive detection and analysis of vulnerabilities in cloud business assets, covering over 100,000 complex vulnerability types. It provides an inventory of affected assets and offers repair suggestions.	
Webpage Risk Assessment	For public network IP and domain name web services, the Cloud Security Center provides webpage tampering, sensitive information, and hidden link detection. It compiles a risk asset list and provides repair suggestions.	
Security Expert Defense Guidance	Based on the results of the above inspection items, security experts provide professional analysis and defensive guidance. After the user has reinforced their security, they can repeat the detection verification within the service validity period.	

Cloud Security Remote Escort Service

Provides users with security alert monitoring during network security attack and defense drills and security assurance in critical periods. It remotely analyzes attack alerts and security experts provide disposal suggestions and defense reports.

Feature Name	Service Content	Deliverables
Abnormal Host	Monitors abnormal terminal attack behaviors such as port blasting, WebShell, command execution, reverse shell,	Daily Defense Report

Security Monitoring	malicious requests, and other attack behaviors such as local privilege escalation after an intrusion.	
Web Intrusion Prevention Monitoring	Monitoring SQL injection, unauthorized access, cross-site scripting (XSS), and other web application layer attack behaviors.	
Network Attack Protection Monitoring	Monitoring internet access, network attacks, abnormal access, scanning behavior, and proactive defense results, as well as lateral spread behavior following an intrusion.	
Leakage Monitoring	Monitoring AccessKey compromise events publicly disclosed on networks such as GitHub.	
Proactive Defense Monitoring	After deploying the Cloud Firewall Network Honeypot, monitor the attacker's entrapment by the honeypot, trace the attacker's information, and incorporate it into the defender's report.	
Judgment Analysis	• Collaborate with customers to analyze attack alerts from cloud security products and provide handling suggestions. • Issuing defense suggestions and incident restoration reports for attack events.	
Emergency response	Emergency response to intrusion events, reconstructing the attack chain and providing disposal suggestions, tracing attacker information, and summarizing defensive actions in a report.	
Defense Summary Service	Summarizes the drill process in a report and provides guidance on fixing issues exposed during the drill.	Defensive Summary Report

Cloud Security Protection Verification Service

Provides users with simulated attack testing services to identify business vulnerabilities and verify the effectiveness of security protection measures, offering an overall security assessment.

Feature Name	Service Content	Deliverables

Standard Protection Verification Service	Applicable to relatively simple operations, security experts conduct penetration tests on domains, mini-programs, and apps. Based on the simulated attack capabilities of the Cloud Security Center BAS, combined with manual simulation, the service attacks the business, uncovers business and configuration vulnerabilities, assesses their security, and delivers a report.	Protection Verification Report
Advanced Protection Verification Service	Applicable to businesses with billing and payment features, security experts conduct penetration tests on domains, mini-programs, and apps. Under the premise of disabling security products or whitelisting, they simulate attacks on the business based on the attack capabilities of the Cloud Security Center BAS, combined with manual simulation. They identify business and configuration vulnerabilities, assess their security, and deliver a report.	
Multi-Dimensional Simulated Attack and Defense Verification Service	Security experts conduct bulk simulated attack tests on group businesses, uncover business vulnerabilities, and assess business security from a practical attack and defense perspective without disabling security products, delivering a protection verification report.	

Billing Overview

The Cloud Security Expert Technical Support Service is purchased on a prepaid basis, and the number of services required is determined based on the user's business scale among other factors. If the business scale is large and multiple services will be consumed daily, please contact us before purchasing to assess the business scale and confirm the number of services to be purchased.

Feature Name	Service Unit Price	Remarks
Cloud Security Inspection Service	10,000 CNY/call	-
Cloud Security Remote Escort Service	5000 CNY/call	If the business scale is large, consuming the service multiple times daily.
Cloud Security Standard Protection	25,000 CNY/call	Charges are based on assets. Each domain/App/mini-program test consumes one instance. The standard protection verification service is

Verification Service		applicable to assets with fewer than 30 interfaces. For more than 30 interfaces, please purchase the advanced protection verification service.
Cloud Security Advanced Protection Verification Service	65,000 CNY/call	
Multi-Dimensional Simulated Attack and Defense Verification Service	60,000 CNY/person/day	You need to contact us for an assessment of asset scale, after which purchases are made based on man-days.

Billing Modes

1. Navigate to the Cloud Security Center purchase page , select **Purchase Security Services Only,** or set the purchase content according to your needs. The system will automatically calculate the required costs for you.
2. Once your selection is complete, click **Place Order Now**. Completing the payment process will successfully finalize your purchase.

Refund

The Cloud Security Expert Technical Support Service does not support refunds without a valid reason. If you have a special reason for requesting a refund, please contact us . We will assess whether a refund is applicable.

Service scope

1. To purchase Cloud Security Remote, you must first purchase the flagship editions of two or more Tencent Cloud security products (Cloud Firewall, Web Application Firewall, Workload Protection, Cloud Security Center).
2. The scope of Cloud Security Remote Service is based on the user's possession of relevant security products, and the specific service range is determined by the specifications of the security products purchased by the user. For instance, for proactive defense monitoring in the Cloud Security Remote Escort Service, users need to purchase the Cloud Firewall Network Honeypot Service in advance.
3. The Cloud Security remote service operates for 8 hours per day, from 9:00 to 17:00. If 24-hour standby service is required, please contact us to increase your purchase.
4. Cloud Security Remote, does not provide judgment analysis services for alarms related to non-Tencent Cloud products and non-Tencent Cloud security products.

5. The scope of Cloud Security Remote Service is limited to the capabilities of the security products that the customer has already purchased. For instance, if the Cloud Firewall does not support MAC address restrictions, then the escort service will not support MAC address restrictions either.
6. Cloud Security Expert Technical Support, offering inspection and escort services exclusively within the scope of the public cloud.