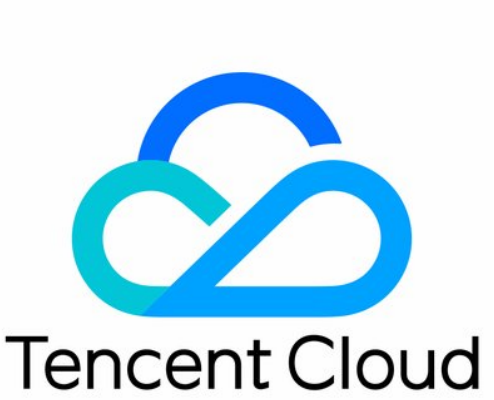
Cloud Workload Protection Platform

Product Introduction



Copyright Notice

Trademark Notice

Tencent Cloud

Service Notice

This document provides an overview of the as-is details of Tencent Cloud's products and services in their entirety or part. The descriptions of certain products and services may be subject to adjustments from time to time.

The commercial contract concluded by you and Tencent Cloud will provide the specific types of Tencent Cloud products and services you purchase and the service standards. Unless otherwise agreed upon by both parties, Tencent Cloud does not make any explicit or implied commitments or warranties regarding the content of this document.

Contact Us

We are committed to providing personalized pre-sales consultation and technical after-sale support. Don't hesitate to contact us at 4009100100 or 95716 for any inquiries or concerns.

Contents

Product Introduction
- Overview
- Advantages
- Use Cases
- Basic Concepts
- Features In Different Editions

Product Introduction
Overview

Last updated: 2025-02-21 14:10:32

What Is Cloud Workload Protection Platform?

Cloud Workload Protection Platform (CWPP) is a security protection product for cloud workloads (supporting both Tencent Cloud and non-Tencent Cloud hosts). Based on the massive threat data accumulated by Tencent Security and utilizing machine learning, it provides security protection services such as hacker intrusion detection and vulnerability risk warning. Key features include password cracking interception, abnormal login alerts, Trojan file detection, and high-risk vulnerability detection. These functions address the main network security risks faced by servers today, helping enterprises build a server security protection system.
Currently, Cloud Workload Protection Platform (CWPP) offers three editions: basic edition protection, professional edition protection, and flagship edition protection. For differences in the main features provided by each edition, please refer to Description of the Feature and Version Comparison.

Why Is Cloud Workload Protection Platform Needed?

Once a server is invaded by hackers, enterprises face the following security risks:

- **Business interruption**: Databases and files are tampered with or deleted, resulting in inaccessible services and system paralysis.
- **Data Theft**: Hackers steal enterprise data and sell it publicly, causing the leakage of customer privacy data, resulting in corporate brand damage and customer loss.
- **Encrypted blackmail**: After hackers intrude into the server, they plant irreversible encryption blackmail software to encrypt the data and extort money from the enterprise.
- **Service instability**: Hackers run mining programs in the server and obtain profit through DDoS Trojan programs, consuming a large amount of system resources, resulting in the server being unable to provide normal services.

Using CWPP can effectively prevent the above issues and ensure the security of enterprise hosts.

Main Features Of Cloud Workload Protection Platform

File Killing

A website backdoor Trojan, also known as a Webshell, is generally a dynamic script such as ASP, PHP, JSP, etc., placed by hackers after invading a website through vulnerabilities. Hackers can continuously control the server through the backdoor Trojan, carry out various destructive actions such as file upload and download, command execution, etc., posing a great threat to website security.
Based on machine learning website backdoor detection technology and relying on Tencent Cloud Security Platform's whole network malicious file sample collection capability, Cloud Workload Protection Platform can accurately detect various types of Trojan malicious files in real time, and also provide malicious file detection and one-click isolation functions to protect the security of your server.

Exceptional Log-In

Analyze the server log-in logs based on four dimensions: common log-in source IP, log-in username, log-in time, and log-in location, so as to identify abnormal log-in behaviors in the log-in flow. Mark the abnormal log-in records as "suspicious" or "high risk" according to the intelligent algorithm, and provide you with real-time alarm notifications.

Password Cracking

Your Cloud Virtual Machine (CVM) can be accessed via the Internet, which gives lawbreakers the opportunity to attempt brute force cracking to intrude into your CVM. Tencent Cloud security detects whether your CVM is being attempted to be brute force cracked through multiple dimensions and various means. If an anomaly is detected, you will be informed through in-site messages or Short Message Service (SMS) and other channels.

Malicious Request

Cloud Workload Protection Platform (CWPP) realizes effective identification of malicious request behaviors through real-time monitoring and processing capabilities for external request behaviors. If malicious request behavior is detected, the CWPP system will provide you with real-time alarm notifications.

High-Risk Command

Based on Tencent Cloud security technology and multi-dimensional means, real-time monitoring of commands in the system is implemented, and the degree of danger of commands can be classified by configuring rules. If high-risk commands are detected, the Cloud Workload Protection Platform (CWPP) system will provide you with real-time alarm notifications.

Local Privilege Escalation

If an event occurs where someone enters the system with low privileges and then uses certain means to elevate their privileges to gain high permissions, it is very likely to be a hacker attack, which can endanger the security of the cloud server. The local privilege escalation feature of the Cloud Workload Protection Platform (CWPP) can monitor privilege escalation events on your server in real-time, and allows you to view and handle the details of these events. It also supports the creation of an allowlist for setting permitted privilege escalation behaviors.

Rebound Shell

The rebound shell feature is based on Tencent Cloud security technology and multi-dimensional means to identify and record reverse connection behaviors of shells on the server, providing real-time monitoring capability for rebound shell behaviors on your cloud server.

Vulnerability Management

CWPP provides real-time alerts for high-risk vulnerabilities on CVMs and offers fixing solutions, including emergency vulnerabilities, Linux Software Vulnerability, Windows System Vulnerability, Web-CMS Vulnerability, and application vulnerabilities, helping enterprises quickly respond to vulnerability risks.

Baseline Management

Tencent Cloud Host Security supports periodic detection and one-click detection of baseline items, supports detection of specified baseline items on specified hosts, supports understanding the baseline pass rate and risk situation through detection policies, and can also provide the risk level and remediation suggestions of baselines and detection items. At the same time, it provides Tencent Cloud's default baseline policy, which helps you better manage the baseline security in your servers.

Advanced Defense

Based on Tencent Cloud security technology, it monitors network attack behaviors in real time and supports the detection of threat types including: webshell detection, struts vulnerability exploitation, code repository pull, code injection attack, command injection attack, and machine batch control utilization, etc.

Security Operations

According to the "Cybersecurity Law," the storage duration of logs should not be less than six months. It is recommended that each server is configured with 30GB of storage capacity for collecting and retaining log data. Log analysis provides multi-dimensional security logs such as Trojan horses, vulnerabilities, and cybersecurity events. It supports statement retrieval and

query, and offers visualization reports, statistical analysis, and export features, enabling you to quickly troubleshoot and trace the source of security events on the host and improve operational efficiency.

Advantages

Last updated: 2025-02-21 14:10:57

The comparative advantages of Tencent Cloud Workload Protection Platform and other host security products are shown in the following table:

Strengths	Tencent Cloud Workload Protection Platform (CWPP)	Other Host Security Products
Hacker behavior detection	**Based on Tencent's network-wide threat data sources, real-time detection of hacker attack behaviors.**	Based on single-machine behavior data for judgment, weak detection capability, unable to respond quickly.
Trojan file detection	**The backend integrates Tencent PC manager's new generation TAV anti-virus engine and hubble analysis system, responding quickly to unknown risks. The WebShell detection engine based on machine learning effectively combats encrypted and deformed malicious scripts.**	Lack of detection capability for executable malicious files, high risk of false alarms and missed reports when detecting WebShell based on regular expressions and character logic matching.
Installation-free, maintenance-free	**Automatically associate Cloud Platform server Ops information, proceed to purchase a CVM and you can use the relevant information immediately. Security policies are automatically updated on the cloud, eliminating the need for Manual Maintenance of various security detection script files.**	Requires the user to log in to the server for manual installation, and a person with certain security technical capability to configure security policies.
Centralized Ops	**Security events can be centrally managed in the console, eliminating the trouble of logging into multiple servers. Host assets are centrally managed, quickly building a security visualization Ops platform.**	Need to log in to the server to handle individual security events.
Low resource	**Self-developed lightweight Agent. The vast majority of computations and protections are carried out on**	The software client has high memory usage, generally consuming more than 100MB,

occupation	**the cloud, resulting in low resource consumption for servers.**	which can affect server performance during peak business hours.

Use Cases

Last updated：2025-02-27 11:49:27

One-Stop Security Management For Enterprise Host Assets

By installing the Cloud Workload Protection Platform (CWPP) client, you can integrate Tencent Cloud Virtual Machines (CVMs) and non-Tencent Cloud servers (third-party cloud servers, on-premises IDC servers) into CWPP for unified security management, leveraging its excellent scalability, adaptability, and stability. It supports 16 types of asset fingerprinting and classification display of TOP5 statistics, helping to visualize corporate assets.

Essential Security Products For Important Protection, Cyber Defense Operation Scenarios, and Attack and Defense Verification

CWPP supports features such as vulnerability defense, file detection and elimination, event investigation, network attack detection, and other host security functions. It provides security protection capabilities in scenarios like critical protection and network defense through defense before events, detection during events, and post-event tracing.

Applicable To Cybersecurity Classified Protection Compliance Scenarios, Essential Products For Cybersecurity Classified Protection

CWPP supports baseline rules such as cybersecurity classified protection level 2, level 3, weak passwords, CIS baseline, and Tencent security standard. It also allows users to customize security baselines.

Basic Concepts

Last updated: 2025-02-27 11:49:42

Security Baseline

A security baseline is a specific set of standards and basic requirements that relevant system and service security configurations must meet to satisfy security needs. Projects of different configurations and policies, such as account configuration security, password configuration security, authorization configuration, log configuration, and network configuration, are used to evaluate whether a product has met the security baseline. The evaluation result reflects the server security to some extent.

Trojan Virus

A Trojan virus is a piece of malicious code or a backdoor program hidden in legitimate applications that has the capability to destroy and delete files, send passwords, record keystrokes, and launch DDoS attacks among others.

WebShell

WebShell is a command execution environment that exists as webpage files such as .asp, .php, .jsp or .cgi files, and is a type of web backdoor. After gaining access to a website, hackers usually mix the backdoor files with the normal webpage files in the WEB directory of the website server, thus gaining access to the asp or php backdoor with the browser, and getting a command execution environment to control the website server.

Host Vulnerability Detection

Host Vulnerability Detection refers to the method of a host agent to detect vulnerabilities on a host. The vulnerability detection module runs on the host and can directly verify or collect information to determine whether the host has vulnerabilities.

Unauthorized Access

Unauthorized access is a type of problems caused by failure to meet the security baseline and mainly refers to the lack of restrictions on the conditions for access to certain services, such as password setting and access source restriction. In this case, anyone can directly connect to the service and perform operations, resulting in security problems.

Abnormal Login

With RDP and SSH login logs collected from the server, information such as login source IP, login username, login time, and login location is reported to the cloud for risk assessment, so

as to send alarms against illegal logins in real time.

File Isolation

Using isolation technology to isolate and store malicious Trojans and virus files to prevent malicious files from continuously spreading.

Features In Different Editions

Last updated: 2025-02-21 14:14:20

Tencent Cloud Workload Protection Platform (CWPP) offers three paid versions to meet different customer needs: inclusive edition, Professional Version, and flagship edition. The main features provided by different versions of CWPP are compared in the table below:

Note:
Due to billing adjustments, Host Security will discontinue the inclusive edition (subscription: 10 CNY/unit/month, only for Tencent Cloud Lighthouse) and the Professional Version (pay-as-you-go: 3 CNY/unit/day) from November 30, 2023. Subsequent new purchases of the inclusive edition and the pay-as-you-go model of the Professional Version will no longer be supported.

- Old inclusive edition orders can still be used and renewed normally.
- Old Professional Version pay-as-you-go orders can still be used and scaled out normally.

Category	Content	Detailed Description	Basic Version (Free)	Universal Edition (Discontinued)	Professional Version (Monthly Subscription: 80 CNY/Instance/Month)	Flagship Edition (Monthly Subscription: 180 CNY/Instance/Month)	Value-Added Service (Separate Billing)
Security Overview	Security Overview	Displays the health score, protection status, pending risks, risk trend, and real-time dynamics of host security.	✓	✓	✓	✓	-
Asset	Asset Das	Displays the statistics of all hosts and asset	×	✓	✓	✓	-

Center	hboard	fingerprints, host overview trend chart, resource monitoring overview, and top 5 accounts, ports, processes, software applications, databases, Web applications, Web services, Web frameworks, and Web sites.					
	Host list	The host list supports classification filtering, viewing protection/risk status, installing/uninstalling clients, and other features for unified management of servers.	✓	✓	✓	✓Detection + Hybrid Cloud + Partial Event Investigation	–
	Asset Fingerprint	Displays the classification list of asset fingerprints, including each asset fingerprint item and its corresponding number of servers. Supports querying and	×	✓Collect 5 kinds of fingerprints	✓Collect 10 kinds of fingerprints	✓Collect 16 kinds of fingerprints	–

		exporting fingerprint data.					
	Security Alerts	Displays asset protection status, security status, CWPP protection, security broadcast, urgent notifications, and hot threat across the entire network in a large screen format. Supports global search.	×	×	×	✓	–
Intrusion Detection	Malicious File Scan	Malicious file: Detects malicious files such as mining Trojans and Ransomware through file scanning.	×Accumulates up to 5 free detections, stops if exceeded	✓Detection + Process Tree	✓Detection + Process Tree	✓Detection + Process Tree + Auto Isolation + Partial Event Investigation	–
		Abnormal process: Detects running abnormal processes through process	×	×	✓Detection	✓Detection	–

	scanning (for Linux systems).					
Password Cracking	• Supports real-time detection, Alarm, and blocking of brute force cracking behaviors for SSH, RDP, etc., and allows allowlist configuration. • Supports custom brute force blocking rules, such as blocking for 15 minutes if there are more than 5 login failures within 1 minute. • Records events, including source IP, source location, login username, attack time, number of attempts, and blocking status.	✓Detection	✓Detection + Auto Blocking	✓Detection + Auto Blocking	✓Detection + Auto Blocking + Partial Event Investigation	–

	Abnormal Login	• Supports real-time monitoring of abnormal login behaviors, identifying non-allowlist IP logins and determining threat levels. • Supports allowlist configuration in terms of source IP, login username, login time, login location, and effective server range.	✓Detection	✓Detection	✓Detection	✓Detection	–
	Malicious Requests	Detects the server's internal or external connection requests with malicious domain names in real time, provides threat source information and event records, and sends alarms automatically to users.	×	×	✓Detection	✓Detection + Automatic Interception + Partial Event Investigation	–
	Local privil	• Real-time monitoring and alarming	×	×	✓Detection +	✓Detection + Proces	–

	ege escalation	for privilege escalation events on your server (entering the host with low privilege and then gaining high-permission through certain actions), with allowlist configuration supported. • Records events, including the server name, privilege escalation user, privilege escalation process, parent process, parent process user, discovery time, file path and process tree.			Process Tree	s Tree + Partial Event Investigation	
	Reverse shell	• Recognizes and alarms for connections established by reverse shell on a public	×	×	✓Detection + Process Tree	✓Detection + Process Tree + Partial Event	–

		network server, and supports allowlist configuration. • Records events, including the server name, connection process, parent process, target server, target port, discovery time, file path, process tree and execution commands.				Investigation	
	High-risk Commands	• Records the bash command executed on the CVM, and monitors potentially dangerous operations aligning with the audit rules in real time. • Provides default rule configuration and supports	×	×	✓Detection + Process Tree	✓Detection + Process Tree + Automatic Interception + Partial Event Investigation	-

		user custom rule configuration. • Records events, including the server name, matched rule name, threat level, command content, login user and operation time.					
Vulnerability Management	Urgent Vulnerability	• Detects recent urgent vulnerabilities (such as zero-day attacks). • Displays vulnerability details, including the vulnerability description, vulnerability type, threat level, fix scheme, reference link, disclosure event, CVE number, CVSS score, and radar chart.	× Detects at most 5 risks for free	✓Detection	✓Detection	✓Detection	–

	Linux Software Vulnerability	• Detects gnutls resource management errors and other common Linux software vulnerabilities and provides fix schemes. • Displays vulnerability details, including the vulnerability description, vulnerability type, threat level, fix scheme, reference link, disclosure event, CVE number, CVSS score, and radar chart.		×	✓Detection	✓Detection and partial fixing	–
	Windows System Vulnerability	• Detects and provides fix schemes for Windows system vulnerabilities by syncing the patch sources on Microsoft's official website in real time, to		×	✓Detection	✓Detection	–

		prevent hackers from attacking or threatening your server through the vulnerabilities. • Displays vulnerability details, including the vulnerability description, vulnerability type, threat level, fix scheme, reference link, disclosure event, CVE number, CVSS score, and radar chart.					
	Web – CMS Vulnerability	• Checks phpMyAdmin, WordPress and other web components for common Web vulnerabilities and provides fix schemes. • Displays vulnerability details, including the vulnerability		×	✓Detection	✓Detection and partial fixing	–

		description, vulnerability type, threat level, fix scheme, reference link, disclosure event, CVE number, CVSS score, and radar chart.					
	Application Vulnerability	• Provides weak password detection for system services, as well as vulnerability detection for system and application services. • Displays vulnerability details, including the vulnerability description, vulnerability type, threat level, fix scheme, reference link, disclosure event, CVE number, CVSS score, and radar chart.		×	✓Detection	✓Detection and partial defense	–

Security baseline	CIS Baseline Standard	• Supports baseline detection for cybersecurity classified protection level 2 and 3, CIS, weak passwords, and provides repair plans. • Displays information on check results under different baseline strategies, including the check server, check items, baseline pass rate, top 5 baseline check items, and top 5 server risks, and supports one-click checks and periodic checks.	× Detects at most 5 risks for free	×	✓Detection	✓Detection + Customization	–
	Cybersecurity Classified Protection Level-2/Level 3			×	✓Detection	✓Detection + Customization	–
	Tencent Cloud Baseline Standard			×	✓Detection	✓Detection + Customization	–
	Weak Password Baseline			✓Detection	✓Detection	✓Detection + Customization	–
Advanced Defense	Java Memory Horse	Monitor in real time and capture unknown classes in the memory of JavaWeb service	×	×	×	✓Detection	–

		processes. Automatically identify memory Trojans using Tencent Cloud's attack and defense experience and expert knowledge. When a Java Webshell is detected, the system will send you real-time alarms.					
	Core File Monitoring	You can configure monitoring rules for core files and view and process monitoring events. You can also configure the allowlist to allow permitted access to files. (Only operating systems with Linux kernel 3.10 or above are supported.)	×	×	×	✓Detection	–
	Network Attack	Perceive malicious attack traffic on the host side, monitor malicious attack behaviors in real time, cover cloud hotspot vulnerabilities,	×	×	✓Detection	✓Detection	–

		and support north-south and east-west attack traffic detection.					
Value-Added Services	Log Analysis	View detailed stored traffic logs, support log retrieval and querying based on retrieval statements, and provide report generation and statistical analysis services.	×Value-Added Billing	×Value-Added Billing	×Value-Added Billing	×Value-Added Billing	Independent billing: 0.5 CNY/GB/month
Settings center	Alarm Settings	Supports alarm notifications via SMS and email, and supports outputting lists of alarm events.	✓	✓	✓	✓	-
	Authorization Management	If you have purchased the CWPP Pro or CWPP Ultimate, you can bind the server to upgrade its protection level on the License Management page. You can also unbind an upgraded server.	✓	✓	✓	✓	-
Performance	Resource occu	Each agent requires low resource usage with CPU usage below 5% and	✓	✓	✓	✓	-

	patio n	memory below 30 MB, which does not affect the system performance.					
	Stab ility requ irem ents	With a high-reliability and high-stability system design, the system can implement mechanisms such as downgrade or suicide when the cloud server encounters an abnormal situation to ensure the normal operation of your business.	✓	✓	✓	✓	-
	Multi - Oper ating Syst em Sup port	Compatible with major operating systems such as Windows, CentOS, Debian, and RedHat.	✓	✓	✓	✓	-