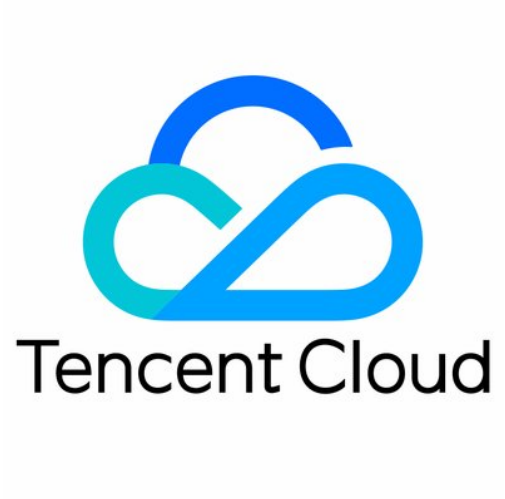
# Cloud Workload Protection Platform

## Product Introduction

## Product Documentation



# Contents

# Product Introduction

# Overview

Last updated：2023-12-26 16:17:43

This document describes the basics of CWPP.

## Overview

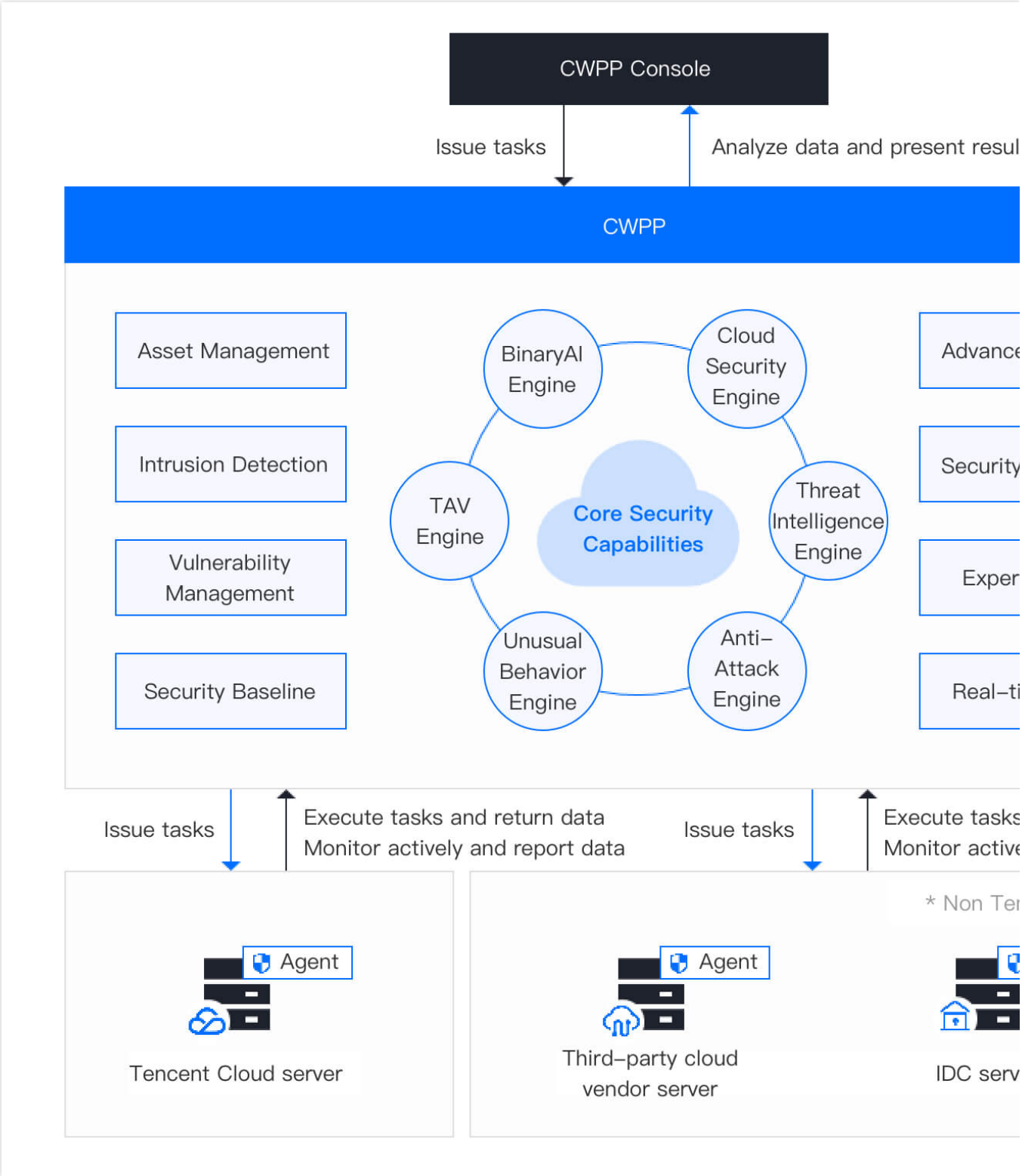
Cloud Workload Protection Platform (CWPP) leverages the massive amount of threat data accumulated by Tencent Security and uses machine learning algorithms to provide security services for servers. It can detect and block brute-force attacks, abnormal logins, Trojan files, high-risk vulnerabilities, and more.

## Qualifications

CWPP has obtained a number of international authoritative certifications such as and CSA CSTR (CSA, Cloud Sec Tech Review).
VB100: Certified 42 times in a row with 100% pass rate
AV-C: 29 A+ ratings, Top Rated product for three consecutive years
Gartner: Listed in the Market Guide for Cloud Workload Protection Platforms
AMTSO: Member of Anti-Malware Testing Standards Organization (AMTSO)
AVAR: Member of Association of Anti-Virus Asia Researchers (AVAR)
EICAR: Member of European Institute for Computer Anti-Virus Research (EICAR)

## How it Works

Install the CWPP agent on the server to .
When you start a detection task on the CWPP console, the agent will execute the task and return data. You can check and process the security events on the CWPP console.




| Term | Description |
| --- | --- |
| CWPP console | A cloud-native security system independently developed by Tencent Cloud,<br> which provides a one-stop cloud workload protection solution (prevention-defense-detection-response). |
| | |

| | |
|---|---|
| Agent | Official security plugin for CWPP, which can be used for servers running in a hybrid cloud.<br> It syncs risk information to CWPP in real time and performs detection or process tasks issued by the CWPP Console. |
| Tencent Cloud servers | CVM, Lighthouse, and ECM. |
| Non-Tencent Cloud servers | Third-party servers and IDC servers. |
| CWPP | Cloud Workload Protection Platform (CWPP) is a security information processing center that continuously checks and analyzes the information returned by different servers. It boasts six core security capabilities to check servers from various dimensions.<br><br>1. TAV Engine: Efficiently detects and removes binary Trojan viruses.<br>2. BinaryAI Engine: The binary search engine built on the deep learning algorithm for efficient detection and removal of malicious samples.<br>3. Cloud Security Engine: Efficiently detects and removes the popular Trojans and virus files both at home and aboard based on the deep self-learning algorithm and multi-engine cloud virus detection mechanism.<br>4. Threat Intelligence Engine: Built on a large threat intelligence library that keeps updated to help identify malicious files, IPs, and domain names.<br>5. Anti-Attack Engine: Detects cyber attacks in real time, including Webshell detection, Struts vulnerability exploitation, code repository pulling, code injection attacks, and brute force cracking. Provides auto defense capabilities.<br>6. Unusual Behavior Engine: Matches unusual behavior characteristics and detects multi-behavior threats in real time to facilitate real-time detection and alarm of malicious intrusion events. |

## Editions

CWPP is available in Basic, Pro and Ultimate editions. For more information on the features in different editions, see Features in Different Editions.

## How to Use

After registering a Tencent Cloud account, you can configure security protection settings on the CWPP Console. For more information about console operations, see Operation Guide.

# Advantages

Last updated：2023-12-26 16:17:58

This document describes the advantages of CWPP.

## Advantages

Tencent Cloud CWPP has the following advantages:

| Advantage | Tencent Cloud CWPP | Other host security products |
| --- | --- | --- |
| Hacking behavior detection | Based on the threat data collected from the entire Internet, CWPP is able to detect hacker attacks in real time. | Determination is made based on the single-server behavior data with weak detection ability and slow response. |
| Trojan file detection | The CWPP backend is integrated with the new-gen TAV anti-virus engine of Tencent PC Manager and the Hubble Analysis System to respond to unknown risks instantly. Its machine learning-based WebShell detection engine can effectively combat encrypted and disguised malicious scripts. | In the absence of the ability to detect executable malicious files, WebShell detection is only conducted based on regular expressions and character logic matching, which can lead to a lot of false positives and false negatives. |
| Installation and ops free | The ops information of cloud platform servers can be automatically associated, which can be used after you purchase a CVM, Lighthouse, or ECM instance. Security policies are automatically updated in the cloud, with no manual maintenance of various security detection scripts required. | You need to log in to individual servers to manually install the product, and personnel with certain security knowledge are required to configure security policies. |
| Centralized management | Security events can be managed in the console in a centralized manner, eliminating your need to log in to multiple servers. Centralized management of server assets enables you to quickly construct a visualized security platform. | You need to log in to individual servers to address security events one by one. |
| Low resource consumption | With self-developed lightweight agents, CWPP carries out most of its computing and protection | Software clients consume a high amount of memory resources (generally over |

| | | |
|---|---|---|
| | workload in the cloud, ensuring low consumption of server resources. | 100 MB), which may compromise server performance during peak hours. |

# Basic Concepts

Last updated：2023-12-26 16:18:06

This document describes the basic concepts of CWPP.

## Basic Concepts

Common concepts of CWPP are as follows.

### 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.

### Vulnerability detection

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

### System component

In a general sense, a component (or common component) at the server layer refers to a web container or software program corresponding to a service or application, such as Nginx and WordPress. A system component mainly refers to non-web system software.

### Common component vulnerability

A common component vulnerability (aka common vulnerability) mainly refers to a vulnerability in a common component instead of business code, such as SQL injection in WordPress and ShellShock in a component's Bash.

### 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

The isolation technology is to isolate and store malicious Trojans and virus files to prevent them from spreading.

# Scenarios

Last updated：2023-12-26 16:18:14

This document describes the common use cases of CWPP.

## Scenarios

When your server is compromised, you will 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 your data and sell it publicly, leading to customer privacy leaks, and thus causing customer churn and damage to your brand image.
File encryption by ransomware: Hackers intrude into your server and implant irreversible ransomware to encrypt your data for ransom.
Service instability: Hackers run mining programs and DDoS Trojans on your server to gain financial benefits, which consumes a large amount of system resources, thus causing the failure of the server to provide services.
CWPP can effectively prevent the above problems and ensure the security of your servers.

# Associated Products

Last updated：2023-12-26 16:18:57

This document describes Tencent Cloud products associated with CWPP.

## Associated Products

The following Tencent Cloud products are involved while using CWPP:

| Tencent Cloud product | CWPP feature involved | Description |
| --- | --- | --- |
| CVM<br>Lighthouse<br>ECM | All features | CVM, Lighthouse, and ECM are all computing services provided by Tencent Cloud and are protected by CWPP. |
| Cloud Block Storage | Vulnerability fix | The auto fix of vulnerabilities feature of CWPP requires snapshot backup, which is supported by CBS. |

# Features in Different Editions

Last updated：2024-05-10 09:41:10

The features of different CWPP editions are listed below.

| Category | Feature | Description | CWPP Basic Free of charge | CWPP Pro Monthly subscription: 12 USD/license/month | CWPP Ultimate Monthly subscription: 27 USD/license/month |
|---|---|---|---|---|---|
| Security Dashboard | Security Dashboard | Displays the health score, protection status, pending risks, risk trend, and new security incidents in real time. | ✓ | ✓ | ✓ |
| Asset Management | Asset Dashboard | Displays the statistics of all servers and asset fingerprints, as well as top 5 accounts, ports, processes, software applications, databases, Web applications, Web services, Web frameworks, and Web sites. | ✓ | ✓ | ✓ |
| | Server List | Displays the information of all servers connected to | ✓ | ✓ | ✓ |

| | | | | | |
|---|---|---|---|---|---|
| | | CWPP, helping you get a full picture of the security status of your assets. | | | |
| | Asset Fingerprint | Provides detailed asset inventory data about server resource monitoring, accounts, ports, and processes and helps you quickly investigate the risks of security events that have occurred. | × | ✓ Supports 10 kinds of fingerprints | ✓ Supports 15 kinds of fingerprints |
| Intrusion Detection | Malicious File Scan | Webshell detection: Detects common web script Trojans and backdoors, covering various script languages such as ASP, PHP, JSP, and Python. Binary virus and Trojan detection: Detects binary executable viruses and | ✓ Detects at most 5 risks for free | ✓ Supports detection (no auto isolation) | ✓ Supports detection, and auto isolation |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Trojans such as DDoS Trojans, remote control, and mining software on .exe, .ddl, and .bin files, and sends alarms. | | | | |
| | Password Cracking | Supports real-time detection, alarm, and blocking of brute force attacks on SSH and RDP, and login allowlist configuration. Supports user-defined blocking rules for brute force attacks, such as rules to detect brute force attacks 5 times within 1 minute and block the attacks detected for 15 minutes. Records events, including the cracking status, server, attacker IP, attack source, login username, | ✓ Supports detection only (no blocking) | ✓ Supports detection and auto blocking | ✓ Supports detection and auto blocking | |

| | | | | | |
|---|---|---|---|---|---|
| | | attack time, number of attack attempts and blocking status. | | | |
| | Unusual Login | Detects logins in real time, and automatically identifies non-allowlist IP logins and malicious logins. Supports allowlist configuration in terms of login source, source IP, server, login username and login time. | ✓ | ✓ | ✓ |
| | 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. | × | ✓ | ✓ |
| | Local Privilege | Supports real-time alarms | × | ✓ | ✓ |

| | | | | | |
|---|---|---|---|---|---|
| | Escalation | for local privilege escalation, and allowlist configuration. Records events, including the server name, privilege escalation user, privilege escalation process, parent process, parent process user, discovery time, file path and process tree. | | | |
| | Reverse Shell | Supports real-time alarms for reverse shells, and 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. | × | ✓ | ✓ |
| | High-risk | Records the | × | ✓ | ✓ |

| | | | | | |
|---|---|---|---|---|---|
| | Commands | bash command executed on the CVM, and monitors potentially dangerous operations aligning with the audit rules in real time. Provides default rules and user-defined rules. 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 | ✓ Detects at most 5 risks for free | ✓ Supports detection (no fixing) | ✓ Supports detection and partial fixing |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | event, CVE number, CVSS score, and radar chart. | | | | |
| | 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. | | | | |
| | 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 | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | 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 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. | | | |
| Security Baseline | CIS Baseline Standard<br>Tencent Cloud Baseline Standard | Supports baseline checks against CIS and weak passwords, and provides fix schemes. | ✓ Detects at most 5 risks for free | ✓ Supports detection (no customization) | ✓ Supports detection and customization |

| | | | | | |
|---|---|---|---|---|---|
| | Weak Password Baseline | Displays check results, including the check server, check items, baseline pass rate, top 5 baseline check items and top 5 server risks, and supports periodic and quick checks. | | | |
| Advanced Defense | 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.) | × | × | ✓ |
| Value-Added Service | Log Analysis | View the details of all stored traffic logs. Log search and query based on search statements are | × Value-added billing | × Value-added billing | × Value-added billing |

| | | | | | |
|---|---|---|---|---|---|
| | | supported. Report and statistical analysis services are provided. | | | |
| Settings | Alarm Notification | Supports alarm notifications via SMS and email, and lists of alarm events. | ✓ | ✓ | ✓ |
| | License 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 Consumption | Each agent requires low resource usage with CPU usage below 5% and memory below 30 MB, which does not affect the system performance. | ✓ | ✓ | ✓ |
| | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | High Stability | With a high-reliability and high-stability system, CVM can implement mechanisms such as downgrade or suicide to ensure the availability of your business. | ✓ | ✓ | ✓ |
| | Multi-Operating System Support | Compatible with major operating systems such as Windows, CentOS, Debian, and RedHat. | ✓ | ✓ | ✓ |