Host Security Service

Service Overview

Issue 19

Date 2025-02-11

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 What Is HSS?

HSS is designed to protect server workloads in hybrid clouds and multi-cloud data centers. It provides host security functions, Container Guard Service (CGS), and Web Tamper Protection (WTP).

HSS can help you remotely check and manage your servers and containers in a unified manner.

HSS protects your system integrity, enhances application security, monitors user operations, and detects intrusions.

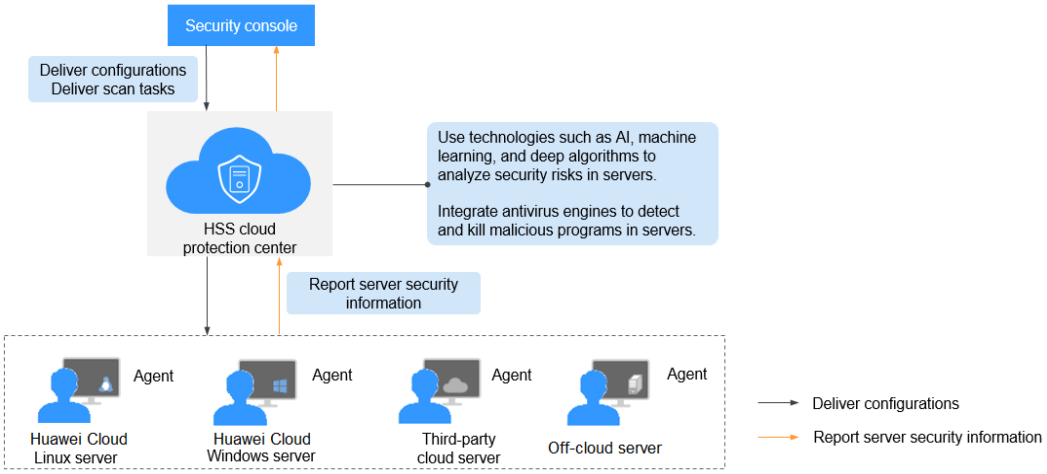
Host Security

Host Security Service (HSS) helps you identify and manage the assets on your servers, eliminate risks, and defend against intrusions and web page tampering. There are also advanced protection and security operations functions available to help you easily detect and handle threats.

Install the HSS agent on your servers, and you will be able to check the server protection status and risks in a region on the HSS console.

Figure 1-1 illustrates how HSS works.

Figure 1-1 Working principles



The following table describes the HSS components.

Table 1-1 Components

Component	Description
Management console	A visualized management platform, where you can apply configurations in a centralized manner and view the protection status and scan results of servers in a region.
HSS cloud protection center	• Analyzes security risks in servers using AI, machine learning, and deep learning algorithms. • Integrates multiple antivirus engines to detect and kill malicious programs in servers. • Receives configurations and scan tasks sent from the console and forwards them to agents on the servers. • Receives server information reported by agents, analyzes security risks and exceptions on servers, and displays the analysis results on the console.
Agent	• Communicates with the HSS cloud protection center via HTTPS and WSS. Port 10180 is used by default. • Scans all servers every early morning; monitors the security status of servers; and reports the collected server information (including non-compliant configurations, insecure configurations, intrusion traces, software list, port list, and process list) to the cloud protection center. • Blocks server attacks based on the security policies you configured. **NOTE** • If no agent is installed or the agent installed is abnormal, the HSS is unavailable. • The agent can be installed on Huawei Cloud Elastic Cloud Servers (ECSs), Bare Metal Servers (BMSs), on-premises IDC servers, and third-party cloud servers. • Select the agent and installation command suitable for your OS. • The HSS agent can be used for all editions, including container security and Web Tamper Protection (WTP). You only need to install the agent once on the same server.

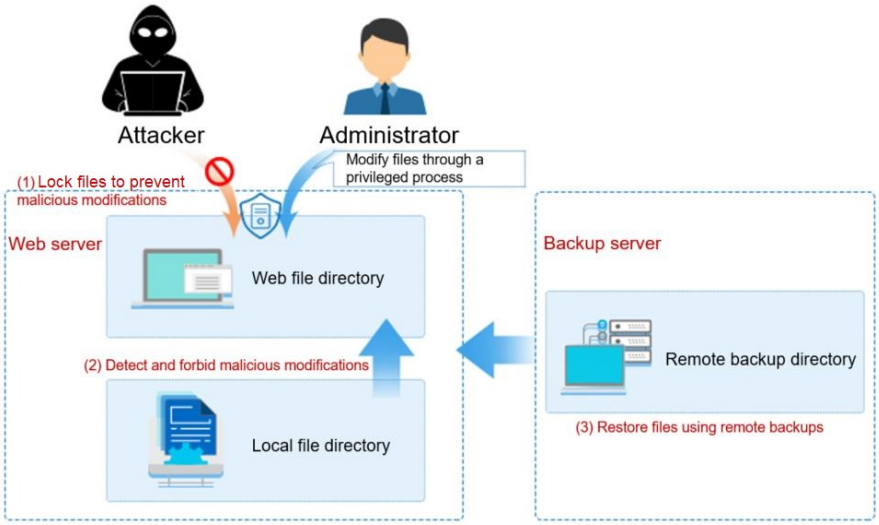
Container Security

HSS provides container security capabilities. The agent deployed on a server can scan the container images on the server, checking configurations, detecting vulnerabilities, and uncovering runtime issues that cannot be detected by traditional security software. Container security also provides functions such as process whitelist, read-only file protection, and container escape detection to minimize the security risks for a running container.

Web Tamper Protection

Web Tamper Protection (WTP) monitors website directories in real time and restores tampered files and directories using their backups. It protects website information, such as web pages, electronic documents, and images, from being tampered with or damaged by hackers.

Figure 1-2 How WTP works



2 Advantages

HSS helps you manage and maintain the security of all your servers and reduce common risks.

Centralized Management

You can check for and fix a range of security issues on a single console, easily managing your servers.

- You can install the agent on Huawei Cloud ECSs, BMSs, on-premises IDC servers, and third-party cloud servers in the same region to manage them all on a single console.
- On the security console, you can view the sources of server risks in a region, handle them according to displayed suggestions, and use filter, search, and batch processing functions to quickly analyze the risks of all servers in the region.

All-Round Protection

HSS protects servers against intrusions by prevention, defense, and post-intrusion scan.

Lightweight Agent

The agent occupies only a few resources, not affecting server system performance.

WTP

- The third-generation web anti-tampering technology and kernel-level event triggering technology are used. Files in user directories can be locked to prevent unauthorized tampering.
- The tampering detection and recovery technologies are used. Files modified only by authorized users are backed up on local and remote servers in real time, and will be used to recover tampered websites (if any) detected by HSS.

3 Scenarios

HSS

- Centralized security management

  With HSS, you can manage the security configurations and events of all your cloud servers on the console, reducing risks and management costs.

- Security risk evaluation

  You can check and eliminate all the risks (such as risky accounts, open ports, software vulnerabilities, and weak passwords) on your servers.

- Account protection

  Take advantage of comprehensive account security capabilities, including prevention, anti-attack, and post-attack scan. You can use 2FA to block brute-force attacks on accounts, enhancing the security of your cloud servers.

- Proactive security

  Count and scan your server assets, check and fix vulnerabilities and unsafe settings, and proactively protect your network, applications, and files from attacks.

- Intrusion detection

  Scan all possible attack vectors to detect and fight advanced persistent threats (APTs) and other threats in real time, protecting your system from their impact.

CGS

- Container image security

  Vulnerabilities will probably be introduced to your system through the images downloaded from Docker Hub or through open-source frameworks.

  You can use CGS to scan images for risks, including image vulnerabilities, unsafe accounts, and malicious files. Receive reminders and suggestions and eliminate the risks accordingly.

- Container runtime security

  Develop a whitelist of container behaviors to ensure that containers run with the minimum permissions required, securing containers against potential threats.

4 Features

HSS comes in basic, professional, enterprise, premium, web tamper protection, and container editions. It provides the following functions: **Dashboard**, **Asset Overview**, **Server Management**, **Container Management**, **Server Fingerprints**, **Container Fingerprints**, **Vulnerability Management**, **Baseline Check**, **Container Image Security**, **Application Protection**, **Web Tamper Protection**, **Ransomware Protection**, **File Integrity Management**, **Virus Scanning**, **Dynamic Port Honeypot**, **Container Firewall**, **Application Process Control**, **Container Cluster Protection**, **Server Alarms**, **Container Alarms**, **Whitelist Management**, **Policy Management**, **Handling History**, **Security Reports**, **Container Audit**, **Installation and Configuration on Servers**. The functions supported by each edition are different. You can select a proper edition based on your service requirements.

- To protect test servers or individual users' servers, use the **basic edition. It can protect any number of servers, but only part of the security scan capabilities are available. This edition does not provide protection capabilities**.
- If you have advanced protection requirements, you are advised to use the premium edition.
- For servers that need to protect websites and key systems from tampering, the **WTP edition** is recommended.
- For containers that need to enhance image security and container runtime security, the container edition is recommended.
- If your servers store important data assets, have high security risks, use publicly available EIPs, or there are databases running on your servers, you are advised to use the **premium or Web Tamper Protection edition**.

NOTICE

- The **enterprise edition** is no longer sold. You are advised to purchase the **premium edition** to protect your server.
- You are advised to **deploy HSS on all your servers** so that if a virus infects one of them, it will not be able to spread to others and damage your entire network.
- After you purchase a protection quota, you can upgrade or switch its edition. For details, see **Upgrading Protection Quotas** and **Switching the HSS Quota Edition**.
- The meanings of the symbols in the table are as follows:
  - √: supported
  - ×: not supported

Dashboard

Dashboard displays the overall security score and protection configuration of assets on the cloud, helping you learn about asset security status.

Table 4-1 Functions

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Dashboard	You can check the security score, risks, and protection overview of all your assets in real time, including servers and containers.	√	√	√	√	√	√

Assets

Asset management displays the asset status and their statistics.

Table 4-2 Assets

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Assets	Collect statistics on asset status and usage of all servers, including the agent status, protection status, quota status, and asset fingerprint.	√	√	√	√	√	√

Servers & Quota

Server management allows you to view and manage servers.

Table 4-3 Server management functions

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Servers & Quota	Manage all server assets, including their protection statuses, quotas, and policies. You can install agents on all the Linux servers in batches.	√	√	√	√	√	√

Containers & Quota

Container management allows you to view and manage servers based on the containers deployed on them, and to manage the security risks of container images and instances.

Table 4-4 Containers & Quota

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Container node management	Manage all container nodes. You can enable or disable protection for container nodes and deploy protection policies.	×	×	×	×	×	√
Container images	Scan local images, third-party repository images, SWR images, and CI/CD images, and check image scan results, vulnerabilities, and the suggestions for fixing abnormal configurations. Detect and resolve image security risks, so that insecure images will not be deployed in the production environment.	×	×	×	×	×	√
Container	Check container instance information and isolate or stop insecure container instances.	×	×	×	×	×	√

Server Fingerprints

Server fingerprints can collect asset information about ports, processes, web applications, web services, web frameworks, and auto-started items on servers. Users can use the server fingerprint function to centrally check asset information on servers and detect unsafe assets in a timely manner.

Table 4-5 Server fingerprint function

Check Item	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Accounts	Check and manage accounts in the current system all in one place. **Supported OSs**: Linux and Windows. **Scan time**: automatic scan every hour.	×	×	√	√	√	√
Open ports	Check open ports all in one place and identify high-risk and unknown ports. **Supported OSs**: Linux and Windows. **Scan time**: automatic scan every 30s.	×	×	√	√	√	√
Processes	Check running applications all in one place and identify malicious applications. **Supported OSs**: Linux and Windows. **Scan time**: automatic scan every hour.	×	×	√	√	√	√
Software	Check and manage server software all in one place and identify insecure versions. **Supported OSs**: Linux and Windows. **Scan time**: automatic scan every day.	×	×	√	√	√	√
Auto-started items	Check auto-started items and collect statistics on their changes in a timely manner. **Supported OSs**: Linux and Windows. **Scan time**: automatic scan every hour.	×	×	√	√	√	√

Check Item	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Web applications	You can check details about software used for web content push and release, including versions, paths, configuration files, and associated processes of all software. **Supported OSs**: Linux and Windows (Tomcat only). **Scan time**: once a week (04:10 a.m. every Monday).	×	×	√	√	√	√
Web services	Check details about the software used for web content access, including versions, paths, configuration files, and associated processes of all software. **Supported OSs**: Linux. **Scan time**: once a week (04:10 a.m. every Monday).	×	×	√	√	√	√
Web frameworks	Check statistics about frameworks used for web content presentation, including their versions, paths, and associated processes. **Supported OSs**: Linux. **Scan time**: once a week (04:10 a.m. every Monday).	×	×	√	√	√	√
Websites	Check statistics about web directories and sites that can be accessed from the Internet. You can view the directories and permissions, access paths, external ports, and key processes of websites. **Supported OSs**: Linux. **Scan time**: once a week (04:10 a.m. every Monday).	×	×	√	√	√	√

Check Item	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Middleware	Check information about servers, versions, paths, and processes associated with middleware. **Supported OSs**: Linux and Windows. **Scan time**: once a week (04:10 a.m. every Monday).	×	×	√	√	√	√
Databases	You can check details about software that provides data storage, including versions, paths, configuration files, and associated processes of all software. **Supported OSs**: Linux and Windows (MySQL only). **Scan time**: once a week (04:10 a.m. every Monday).	×	×	√	√	√	√
Kernel modules	Check information about all the program module files running in kernels, including associated servers, version numbers, module descriptions, driver file paths, file permissions, and file hashes. **Supported OSs**: Linux. **Scan time**: once a week (04:10 a.m. every Monday).	×	×	√	√	√	√

Container Fingerprints

Container fingerprints collect asset information such as accounts, ports, processes, clusters, services, and workloads in containers. You can use the container fingerprint function to centrally check asset information in containers and detect unsafe assets in a timely manner.

Table 4-6 Asset fingerprints

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Account	Check and manage container accounts all in one place. **Supported OSs**: Linux. **Scan time**: automatic scan every hour.	×	×	×	×	×	√
Open ports	Check container open ports all in one place and identify high-risk and unknown ports. **Supported OSs**: Linux. **Scan time**: automatic scan every 30s.	×	×	×	×	×	√
Process	Check running applications all in one place and identify malicious applications. **Supported OSs**: Linux. **Scan time**: automatic scan every hour.	×	×	×	×	×	√
Installed software	Check and manage container software all in one place and identify insecure versions. **Supported OSs**: Linux. **Scan time**: automatic scan every day.	×	×	×	×	×	√
Auto-started items	Check auto-started items and collect statistics on their changes in a timely manner. **Supported OSs**: Linux. **Scan time**: automatic scan every hour.	×	×	×	×	×	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Web application	You can check details about software used for web content push and release, including versions, paths, configuration files, and associated processes of all software. **Supported OSs**: Linux. **Scan time**: once a week (04:10 a.m. every Monday).	×	×	×	×	×	√
Web service	You can check details about the software used for web content access, including versions, paths, configuration files, and associated processes of all software. **Supported OSs**: Linux. **Scan time**: once a week (04:10 a.m. every Monday).	×	×	×	×	×	√
Web frameworks	You can check statistics about frameworks used for web content presentation, including their versions, paths, and associated processes. **Supported OSs**: Linux. **Scan time**: once a week (04:10 a.m. every Monday).	×	×	×	×	×	√
Website	Check statistics about web directories and sites that can be accessed from the Internet. You can view the directories and permissions, access paths, external ports, and key processes of websites. **Supported OSs**: Linux. **Scan time**: once a week (04:10 a.m. every Monday).	×	×	×	×	×	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Middleware	You can also check information about servers, versions, paths, and processes associated with middleware. **Supported OSs**: Linux. **Scan time**: once a week (04:10 a.m. every Monday).	×	×	×	×	×	√
Database	You can check details about software that provides data storage, including versions, paths, configuration files, and associated processes of all software. **Supported OSs**: Linux. **Scan time**: once a week (04:10 a.m. every Monday).	×	×	×	×	×	√
Clusters	Collect statistics on and display cluster details. You can view the type, node, version, and status of all clusters. **Supported OSs**: Linux. **Scan time**: manual scan at any time.	×	×	×	×	×	√
Services	Collect statistics on and display details about services and breakpoints. You can view information about all services, such as namespaces and clusters to which the services belong. **Supported OSs**: Linux. **Scan time**: manual scan at any time.	×	×	×	×	×	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Workloads	Collect statistics on and display details about workloads (StatefulSets, deployments, DaemonSets, normal jobs, cron jobs, and container groups). You can view the status, number of instances, and namespace of all workloads. **Supported OSs**: Linux. **Scan time**: manual scan at any time.	×	×	×	×	×	√
Container instances	Collect statistics on and display container instance details. You can view the status, pods, and clusters of all container instances. **Supported OSs**: Linux. **Scan time**: manual scan at any time.	×	×	×	×	×	√

Vulnerability Management

Vulnerability management detects Linux software vulnerabilities, Windows system vulnerabilities, Web-CMS vulnerabilities, application vulnerabilities and emergency vulnerabilities, helping users identify potential risks.

Table 4-7 Vulnerabilities

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Linux vulnerability detection	Based on the vulnerability database, check and handle vulnerabilities in the software (such as kernel, OpenSSL, vim, glibc) you obtained from official Linux sources and have not compiled. **Supported OSs**: Linux. **Scan time**: automatic scan (every day by default), scheduled scan (once a week by default, not supported in the basic edition), and manual scan at any time (not supported in the basic edition).	√	√	√	√	√	√
Windows vulnerability detection	Detect vulnerabilities in Windows OS based on the official patch releases of Microsoft. **Supported OSs**: Windows. **Scan time**: automatic scan (every day by default), scheduled scan (once a week by default, not supported in the basic edition), and manual scan at any time (not supported in the basic edition).	√	√	√	√	√	×
Web-CMS vulnerability detection	Scan for Web-CMS vulnerabilities in web directories and files. **Supported OSs**: Linux and Windows. **Scan time**: automatic scan (every day by default), scheduled scan (once a week by default), and manual scan at any time.	×	√	√	√	√	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Application vulnerability detection	Detect vulnerabilities in JAR packages, ELF files, and other files of open source software, such as Log4j and spring-core. **Supported OSs**: Linux and Windows. **Scan time**: automatic scan (every Monday by default), scheduled scan (once a week by default), and manual scan at any time.	×	×	√	√	√	√
Emergency vulnerability detection	Checks whether the software and any dependencies running on the server have vulnerabilities through version comparison and POC verification. Reports risky vulnerabilities to the console and provides vulnerability alarms for you. **Supported OSs**: Linux and Windows. **Scan time**: scheduled scan (which needs to be manually enabled) and manual scan at any time.	×	√	√	√	√	√

Baseline Inspection

Baseline inspection can scan risky configurations, weak passwords, and password complexity policies of server systems and key software. The supported detection baselines include security practices. You can customize sub-baseline items and fix vulnerability risks.

Table 4-8 Baseline checks

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Password complexity policies	Check password complexity policies and modify them based on suggestions provided by HSS to improve password security. **Supported OSs**: Linux. **Scan time**: automatic scan in the early morning every day and manual scan at any time.	√	√	√	√	√	√
Common weak passwords	Change weak passwords to stronger ones based on HSS scan results and suggestions. **Supported OSs**: Linux and Windows. **Scan time**: automatic scan in the early morning every day and manual scan at any time.	√	√	√	√	√	√
Unsafe configuration	Check the unsafe Tomcat, Nginx, and SSH login configurations found by HSS. **Supported OSs**: Linux and Windows. **Scan time**: automatic scan in the early morning every day and manual scan at any time.	×	×	√	√	√	√

Container Image Security

Container image security allows you to scan the image repository and running container images, detect vulnerabilities and malicious files in the images, and provide repair suggestions, helping you obtain secure images.

Table 4-9 Container images

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
SWR image repository vulnerabilities	Detect system and application vulnerabilities in SWR image repository based on a vulnerability database and handle critical vulnerabilities in a timely manner. **Supported OSs**: Linux. **Scan time**: manual scan at any time.	×	×	×	×	×	√
Viewing Malicious File Detection Results	Scan images for malicious files (such as Trojans, worms, viruses, and adware) and identify risks. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√

Application protection

Application protection provides security defense for running applications. You simply need to add probes to applications, without having to modify application files.

Table 4-10 Application protection

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
SQL injection	Detect and defend against SQL injection attacks, and check web applications for related vulnerabilities. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
OS command injection	Detect and defend against remote OS command injection attacks and check web applications for related vulnerabilities. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√
XSS	Detect and defend against stored cross-site scripting (XSS) injection attacks. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√
Log4j RCE vulnerability	Detect and defend against remote code execution and intercept attacks. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√
Web shell upload	Detect and defend against attacks that upload dangerous files, change file names, or change file name extension types; and check web applications for related vulnerabilities. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√
Memory injection	Detect and defend against memory injection attacks. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
XXE	Detect and defend against XML External Entity Injection (XXE) attacks, and check web applications for related vulnerabilities. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√
Deserialization input	Detect deserialization attacks that exploit unsafe classes. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√
File directory traversal	Check whether sensitive directories or files are accessed. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√
Struts2 OGNL	Detect OGNL code execution. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√
Command execution using JSP	Detect command execution using JSP. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
File deletion using JSP	Detect file deletion using JSP. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√
Database connection exception	Detect authentication and communication exceptions thrown by database connections. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√
0-day vulnerability	Check whether the stack hash of a command is in the whitelist of the web application. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√
SecurityManager permission exception	Detect exceptions thrown by SecurityManager. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√
JNDI injection	Detect and defend against JNDI injection attacks, and check web applications for related vulnerabilities. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Expression injection	Detect and defend against expression injection attacks, and check web applications for related vulnerabilities. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√

Web Tamper Protection (WTP)

WTP can detect and prevent tampering of files in specified directories, including web pages, documents, and images, and quickly restore them using valid backup files.

Table 4-11 Web Tamper Protection

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Static WTP	Protect the static web page files on website servers from being tampered with. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	×	√	×
Dynamic WTP	Provide dynamic web tamper protection for Tomcat. Protect the dynamic web pages in website databases from being tampered with. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	√	×

Ransomware prevention

Ransomware prevention supports user-defined ransomware prevention policies, using static and dynamic honeypots to identify attacks launched by known and unknown ransomware.

Table 4-12 Ransomware prevention

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Ransomware prevention	Help you identify some unknown ransomware attacks by using static and dynamic honeypot files. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√

Application Process Control

Application process control can detect malicious processes and generate alarms.

Table 4-13 Application process control

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Application Process Control	Learn the characteristics of application processes on servers and manage their running. Suspicious and trusted processes are allowed to run, and alarms are generated for malicious processes. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√

Checking File Integrity

File integrity management checks and records changes to key files.

Table 4-14 File integrity monitoring

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Monitor file integrity	Check the key files of the Linux system to detect the changes that may be exploited by attacks in a timely manner. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√	√

Virus Scan

Virus scan can detect virus files on the server, helping users eliminate potential malicious threats.

Table 4-15 Virus scan

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Virus scan	The function uses the virus detection engine to scan virus files on the server. The scanned file types include executable files, compressed files, script files, documents, images, and audio and video files. Users can perform quick scan and full-disk scan on the server as required. Customize scan tasks and handle detected virus files in a timely manner to enhance the virus defense capability of the service system. **Supported OSs**: Linux and Windows. **Scan time**: manual scan at any time.	×	√ (Only quick scan is supported.)	√	√	√	√

Dynamic Port Honeypot

The **dynamic port honeypot** function uses real ports as bait ports to induce attackers to access the intranet. In the horizontal penetration scenario, the function can effectively detect attackers' scanning and identify faulty servers.

Table 4-16 Function

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Dynamic Port Honeypot	The dynamic port honeypot function is a deception trap. It uses a real port as a bait port to induce attackers to access the network. In the horizontal penetration scenario, the function can effectively detect attackers' scanning, identify faulty servers, and protect real resources of the user. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√

Container Firewalls

Container firewalls protect container runtime.

Table 4-17 Container firewall

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Container Firewalls	Control and intercept network traffic inside and outside a container cluster to prevent malicious access and attacks. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√

Container Cluster Protection

Container cluster protection can detect non-compliant baselines issues, vulnerabilities, and malicious files in images to prevent insecure container images from being deployed in clusters.

Table 4-18 Container cluster protection

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Container cluster protection	Check for non-compliance baseline issues, vulnerabilities, and malicious files when a container image is started and report alarms on or block container startup that has not been unauthorized or may incur high risks. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√

Server Alarms

Server intrusion detection identifies and prevents intrusion to servers, discover risks in real time, detect and kill malicious programs, and identify web shells and other threats.

Table 4-19 Server alarm function

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Unclassified malware	Check and handle detected malicious programs all in one place, including web shells, Trojan, mining software, worms, and viruses. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√	√
Viruses	Check servers in real time and report alarms for viruses detected on servers. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√	√
Worms	Detect and kill worms on servers and report alarms. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√	√
Trojans	Detect programs that are hidden in normal programs and have special functions such as damaging and deleting files, sending passwords, and recording keyboards. If a program is detected, an alarm is reported immediately. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Botnets	Detect whether zombie programs that have been spread exist in servers and report alarms immediately after detecting them. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√	√
Backdoors	Detect web shell attacks in the server system in real time and report alarms immediately after detecting them. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√	√
Rootkits	Detect server assets and report alarms for suspicious kernel modules, files, and folders. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√	√
Ransomware	Check for ransomware in web pages, software, emails, and storage media. Ransomware can encrypt and control your data assets, such as documents, emails, databases, source code, images, and compressed files, to leverage victim extortion. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Hacker tools	Check whether non-standard tool used to control the server exist and report alarms immediately after detecting them. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	√	√	√	√
Webshell	Check whether the files (often PHP and JSP files) detected by HSS in your web directories are web shells. ● Web shell information includes the Trojan file path, status, first discovery time, and last discovery time. You can choose to ignore warning on trusted files. ● You can use the manual detection function to detect web shells on servers. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√	√
Mining software	Detect whether mining software exists on servers in real time and report alarms for the detected software. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Remote code execution	Check whether the server is remotely called in real time and report an alarm immediately once remote code execution is detected. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	√	√	√	√
Redis vulnerability exploits	Detect the modifications made by the Redis process on key directories in real time and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√	√
Hadoop vulnerability exploits	Detect the modifications made by the Hadoop process on key directories in real time and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√	√
MySQL vulnerability exploits	Detect the modifications made by the MySQL process on key directories in real time and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Reverse shells	Monitor user process behaviors in real time to report alarms on and block reverse shells caused by invalid connections. Reverse shells can be detected for protocols including TCP, UDP, and ICMP. Currently, the following types of reverse shells can be blocked: exec reverse shell, Perl reverse shell, AWK reverse shell, Python reverse shell.b, Python reverse shell.a, Lua reverse shell, mkfifo/openssl reverse shell, PHP reverse shell, Ruby reverse shell, rssocks reverse proxy, Bash reverse shell, Ncat reverse shell, exec redirection reverse shell, Node reverse shell, Telnet dual-port reverse shell, nc reverse shell, Socat reverse shell, rm/mkfifo/sh/nc reverse shell, and socket/tchsh reverse shell. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
	NOTE To enable automatic reverse shell blocking, ensure the following conditions are met: 1. In the **HIPS Detection** policy, **Automatic Blocking** is enabled. This function is disabled by default. You need to manually enable it. For details, see **Configuring Policies**. 2. Ensure the function of isolating and killing malicious programs is enabled. This function is disabled by default. You need to manually enable it. For details, see **Enabling Malicious Program Isolation and Killing**..						
File privilege escalation	Check the file privilege escalations in your system. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√	√
Process privilege escalations	The following process privilege escalation operations can be detected: • Root privilege escalation by exploiting SUID program vulnerabilities • Root privilege escalation by exploiting kernel vulnerabilities **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Important file changes	Receive alarms when critical system files are modified. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√	√
File/Directory change	Monitor system files and directories in real time and generate alarms if such files are created, deleted, moved, or if their attributes or content are modified. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√	√
Abnormal process behaviors	Check the processes on servers, including their IDs, command lines, process paths, and behavior. Send alarms on unauthorized process operations and intrusions. The following abnormal process behavior can be detected: ● Abnormal CPU usage ● Processes accessing malicious IP addresses ● Abnormal increase in concurrent process connections **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	√	√	√	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
High-risk command executions	Check executed commands in real time and generate alarms if high-risk commands are detected. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√	√
Abnormal shells	Detect actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√	√
Sensitive file access detection	Detect the unauthorized access to or modifications of sensitive files. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√	√
Suspicious crontab tasks	Check and list auto-started services, scheduled tasks, pre-loaded dynamic libraries, run registry keys, and startup folders. You can get notified immediately when abnormal automatic auto-start items are detected and quickly locate Trojans. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
System protection disabling	Detect the preparations for ransomware encryption: Disable the Windows defender real-time protection function through the registry. Once the function is disabled, an alarm is reported immediately. **Supported OSs**: Windows. **Scan time**: real-time detection.	×	×	√	√	√	×
Backup deletion	Detect the preparations for ransomware encryption: Delete backup files or files in the **Backup** folder. Once backup deletion is detected, an alarm is reported immediately. **Supported OSs**: Windows. **Scan time**: real-time detection.	×	×	√	√	√	√
Suspicious registry operation	Detect operations such as disabling the system firewall through the registry and using the ransomware **Stop** to modify the registry and write specific strings in the registry. An alarm is reported immediately when such operations are detected. **Supported OSs**: Windows. **Scan time**: real-time detection.	×	×	√	√	√	√
System log deletion	An alarm is generated when a command or tool is used to clear system logs. **Supported OSs**: Windows. **Scan time**: real-time detection.	×	×	√	√	√	×

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Suspicious command executions	• Check whether a scheduled task or an automated startup task is created or deleted by running commands or tools. • Detect suspicious remote command execution. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	√	√	√	√
Suspicious process execution	Detect and report alarms on unauthenticated or unauthorized application processes. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	√	√	√	√
Suspicious process file access	Detect and report alarms on the unauthenticated or unauthorized application processes accessing specific directories. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	√	√	√	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Brute-force attacks	Check for brute-force attack attempts and successful brute-force attacks. • Detect password cracking attacks on accounts and block attacking IP addresses to prevent server intrusion. • Trigger an alarm if a user logs in to the server by a brute-force attack. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	√	√	√	√	√	√
Abnormal logins	Check and handle remote logins. If a user's login location is not any common login location you set, an alarm will be triggered. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	√	√	√	√	√	√
Invalid accounts	Scan accounts on servers and list suspicious accounts in a timely manner. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√	√
User account added	Detect the commands used to create hidden accounts. Hidden accounts cannot be found in the user interaction interface or be queried by commands. **Supported OSs**: Windows. **Scan time**: real-time detection.	×	×	√	√	√	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Password thefts	Detect the abnormal obtaining of hash value of system accounts and passwords on servers and report alarms. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	√	√	√	√
Unknown network access	Detect access to ports that are not listened on by the server. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	×	×	√	√	√
Cloud honeypot	An alarm is reported if a connection to the honeypot port of a server is detected.	×	×	×	√	√	×
Abnormal outbound connections	Report alarms on suspicious IP addresses that initiate outbound connections. **Supported OSs**: Linux (kernel 5.10 or later). **Scan time**: real-time detection.	×	√	√	√	√	√
Port forwarding	Report alarms on port forwarding using suspicious tools. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√	√
Suspicious download request	An alarm is generated when a suspicious HTTP request that uses system tools to download programs is detected. **Supported OSs**: Windows. **Scan time**: real-time detection.	×	×	√	√	√	×

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Suspicious HTTP request	An alarm is generated when a suspicious HTTP request that uses a system tool or process to execute a remote hosting script is detected. **Supported OSs**: Windows. **Scan time**: real-time detection.	×	×	√	√	√	×
Port scan	Detect scanning or sniffing on specified ports and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	√	√	√
Host scan	Detect the network scan activities based on server rules (including ICMP, ARP, and nbtscan) and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	√	√	√
Process injection	Scan for malicious code injection into running processes and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√	√
Dynamic library injection	Scan for the payloads injected by hijacking functions in the dynamic link library (DLL) and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Memory file process	Scan for the behaviors of creating an anonymous malicious file that exists only in the RAM through the memfd_create system call and executing the file, and report alarms on such behaviors. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	√	√	√	√	√

Container Alarms

Container alarms can detect intrusion behaviors of Docker and Containerd engines. Scan running containers for malicious programs including miners and ransomware; detect non-compliant security policies, file tampering, and container escape; and provide suggestions.

Table 4-20 Container alarm function

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Unclassified malware	Check and handle malicious programs in a container, including web shells, Trojan, mining software, worms, and viruses. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
Viruses	Check containers in real time and report alarms for viruses detected in the container runtime. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Worms	Detect and kill worms in container runtime and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
Trojans	Detect programs that are hidden in normal programs and have special functions such as damaging and deleting files, sending passwords, and recording keyboards. If a suspicious program is detected, an alarm is reported immediately. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
Botnets	Check for zombie programs spreading in the container runtime and report alarms immediately after detecting them. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
Backdoors	Detect web shell attacks in the container runtime in real time and report alarms immediately after detecting them. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Rootkits	Check the container runtime and report alarms for suspicious kernel modules, files, and folders. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
Ransomware	Check and handle alarms on ransomware in containers. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
Hacker tools	Check for non-standard tools used to control containers in the container runtime, and report alarms immediately after detecting them. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	√	√	√	√
Webshell	Check whether the files (often PHP and JSP files) in the web directories on containers are web shells. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
Mining software	Check for mining software in the container runtime in real time and report alarms for the detected software. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Vulnerability escape detection	An escape alarm is reported if a container process behavior that matches the behavior of known vulnerabilities is detected. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
File escape detection	An alarm is reported if a container process is found accessing a key file directory (for example, **/etc/shadow** or **/etc/crontab**). Directories that meet the container directory mapping rules can also trigger such alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
Reverse shells	Monitor user process behaviors in a container environment in real time to detect reverse shells caused by invalid connections. Reverse shells can be detected for protocols including TCP, UDP, and ICMP. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
File privilege escalation	Check the file privilege escalations in the container system. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Process privilege escalations	The following process privilege escalation operations can be detected: • Root privilege escalation by exploiting SUID program vulnerabilities • Root privilege escalation by exploiting kernel vulnerabilities **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
Important file changes	Receive alarms when critical system files are modified. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
File/ Directory change	Monitor system files and directories in real time and generate alarms if such files are created, deleted, moved, or if their attributes or content are modified. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Abnormal process behaviors	Check the processes on servers in a container environment, including their IDs, command lines, process paths, and behavior. Send alarms on unauthorized process operations and intrusions. The following abnormal process behavior can be detected: • Abnormal CPU usage • Processes accessing malicious IP addresses • Abnormal increase in concurrent process connections **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
Abnormal container processes	• Malicious container program detection Monitor container process behavior and process file fingerprints. An alarm is reported if it detects a process whose behavior characteristics match those of a predefined malicious program. • Abnormal processes The service reports an alarm if it detects that a process not in the whitelist is running in the container. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Abnormal container startup detection	The service monitors container startups and reports an alarm if it detects that a container with too many permissions is started. Container check items include: • Privileged container startup (**privileged:true**) • Too many container capabilities (**capability:[xxx]**) • Seccomp not enabled (**seccomp=unconfined**) • Container privilege escalation (**no-new-privileges:false**) • High-risk directory mapping (**mounts:[...]**) **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
High-risk command executions	Check executed commands in containers and generate alarms if high-risk commands are detected. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
High-risk system calls	You can run tasks in kernels by Linux system calls. The container edition reports an alarm if it detects a high-risk call. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Abnormal shells	Check containers for actions on abnormal shells, including moving, copying, and deleting shell files, and modifying the access permissions and hard links of the files. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
Sensitive file access detection	The service monitors the container image files associated with file protection policies, and reports an alarm if the files are modified. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
Container image blocking	If a container contains insecure images specified in **Suspicious Image Behaviors**, an alarm will be generated and the insecure images will be blocked before a container is started in Docker. **Supported OSs**: Linux. **Scan time**: real-time detection. **NOTE** You need to **install the Docker plug-in**.	×	×	×	×	×	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Suspicious command executions	• Check whether a scheduled task or an automated startup task is created or deleted by running commands or tools. • Detect suspicious remote command execution. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
Abnormal runtime behaviors	Detect container escapes at the levels of networks, servers, pods, containers, processes, and system calls. Five types of abnormal runtime behaviors (processes, files, network activities, process capabilities, and system calls) can be detected, reported, and blocked to prevent container escape and protect container runtime. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Brute-force attacks	Detect and report alarms for brute-force attack behaviors, such as brute-force attack attempts and successful brute-force attacks, on containers. Detect SSH, web, and Enumdb brute-force attacks on containers. **Supported OSs**: Linux. **Scan time**: real-time detection. **NOTE** Currently, brute-force attacks can be detected only in the Docker runtime.	×	×	×	×	×	√
Invalid accounts	Detect suspicious accounts and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
Password thefts	Detect the abnormal obtaining of hash value of system accounts and passwords on servers in a container environment and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
Abnormal outbound connections	Report alarms on suspicious IP addresses in a container environment that initiate outbound connections. **Supported OSs**: Linux (kernel 5.10 or later). **Scan time**: real-time detection.	×	×	×	×	×	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Port forwarding	Report alarms on port forwarding using suspicious tools in a container environment. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
Kubernetes event deletions	Detect the deletion of Kubernetes events and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
Abnormal pod behaviors	Detect abnormal operations such as creating privileged pods, static pods, and sensitive pods in a cluster and abnormal operations performed on existing pods and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
User information enumerations	Detect the operations of enumerating the permissions and executable operation list of cluster users and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
Binding cluster roles	Detect operations such as binding or creating a high-privilege cluster role or service account and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Process injection	Scan for malicious code injection into running processes and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
Dynamic library injection	Scan for the payloads injected by hijacking functions in the dynamic link library (DLL) and report alarms. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√
Memory file process	Scan for the behaviors of creating an anonymous malicious file that exists only in the RAM through the memfd_create system call and executing the file, and report alarms on such behaviors. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√

Whitelist Management

The whitelist function includes **Alarm whitelist**, **Login whitelist** and **System user whitelist**. To reduce false alarms, import events to and export events from the whitelist.

Table 4-21 Whitelists

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Alarm whitelist	You can add an alarm to the whitelist when handling it. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	√	√	√	√	√	√
Login Whitelist	Add IP addresses and usernames to the Login Whitelist as needed. HSS will not report alarms on the access behaviors of these IP addresses and users. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	√	√	√	√	√	√
System user whitelist	Users (non-root users) that are newly added to the root user group on a server can be added to the system user whitelist. HSS will not report risky account alarms for them. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	√	√	√	√	√	√

Policy Management

You can configure **policy management**, customize detection rules, and apply different policies to different servers, containers, or groups, easily adapting to your business scenarios.

Table 4-22 Policies

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Policy Management	You can define and issue different detection policies for different servers or server groups, implementing refined security operations. • Check the policy group list. • Create a policy group based on default and existing policy groups. • Define a policy. • Edit or delete a policy. • Modify or disable policies in a group. • Apply policies to servers in batches on the **Servers & Quota** page. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√ (Only the default professional policy group is supported.)	√ (Only the default enterprise policy group is supported.)	√	√	√

Viewing the Handling History

Handling history displays the handling history of vulnerabilities, viruses, and security alarms.

Table 4-23 Handling history

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Handling history	Check historical vulnerability, virus, and alarm handling records, including the handling time and handlers.	×	√	√	√	√	√

Security Report

The HSS can generate **Security reports** on user assets on a daily, weekly, or monthly basis.

Table 4-24 Security report

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Security Report	Check weekly or monthly server security trend, key security events, and risks.	×	√	√	√	√	√

Container Audit

Container audit monitors and records operations and activities of cluster containers, independent containers, and the image repositories of SoftWare Repository for Container (SWR). You can view and analyze their logs on the HSS console.

Table 4-25 Container audit

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Container audit	Keep track of the operations and activities in your container clusters, gaining insight into every phase of the container lifecycle, including creating, starting, stopping, and destroying containers; as well as the communication and transmission between containers. Find and handle security problems through audit and analysis in a timely manner, ensuring the security and stability of container clusters. **Supported OSs**: Linux. **Scan time**: real-time detection.	×	×	×	×	×	√

Installation and Configuration on Servers

Installation and configuration provides functions such as agent management, common login locations, common login IP addresses, SSH login IP address whitelist, automatic isolation and removal of malicious programs, two-factor authentication, alarm configuration, and container installation and configuration to meet server and container security requirements in different scenarios.

Table 4-26 Installation and configuration

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Agent management	You can view the agent status of all servers and upgrade, uninstall, and install agents. **Supported OSs**: Linux and Windows.	√	√	√	√	√	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Common login location	For each server, you can configure the locations where users usually log in from. The service will generate alarms on logins originated from locations other than the configured common login locations. A server can be added to multiple login locations. **Supported OSs**: Linux and Windows.	√	√	√	√	√	√
Common login IP address	For each server, you can configure the IP addresses where users usually log in from. The service will generate alarms on logins originated from IP addresses other than the configured common IP addresses. **Supported OSs**: Linux and Windows.	√	√	√	√	√	√
Configuring an SSH Login IP Address Whitelist	The SSH login whitelist controls SSH access to servers to prevent account cracking. After you configure the whitelist, SSH logins will be allowed only from whitelisted IP addresses. **Supported OSs**: Linux.	√	√	√	√	√	√
Malicious program isolation and removal	HSS automatically isolates and kills identified malicious programs, such as web shells, Trojans, and worms, removing security risks. **Supported OSs**: Linux and Windows. **Scan time**: real-time detection.	×	√	√	√	√	√

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition
Two-factor Authentication (2FA)	Prevent brute-force attacks by using password and SMS/email authentication. **Supported OSs**: Linux and Windows.	Pay per use: × Yearly/Monthly: √	√	√	√	√	√
Plug-in management	Install, uninstall, upgrade, and manage plug-ins in a unified manner. **Supported OSs**: Linux.	×	×	×	×	×	√
Container installation and configuration	Connect your clusters to HSS. Upgrade or uninstall the agent in your clusters or independent containers. **Supported OSs**: Linux.	√	√	√	√	√	√

HSS Self-protection

Self-protection protects HSS files and processes.

Table 4-27 HSS self-protection

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition

Windows self-protection	Prevent malicious programs from uninstalling the agent, tampering with HSS files, or stopping HSS processes.
	Supported OSs: Windows.
	NOTE
	• Self-protection depends on antivirus detection, HIPS detection, and ransomware protection. It takes effect only when more than one of the three functions are enabled.
	• Enabling the self-protection policy has the following impacts:
	  • The agent cannot be uninstalled on the control panel of a server, but can be uninstalled on the HSS console.
	  • HSS processes cannot be terminated.
	  • In the agent installation path **C:\Program Files\HostGuard**, you can only access the **log** and **data** directories (and the **upgrade** directory, if your agent has been upgraded).
		×	×	×	√	√	×

Function	Description	Basic Edition	Professional Edition	Enterprise Edition	Premium Edition	WTP Edition	Container Edition

Linux self-protection	Prevent malicious programs from stopping the HSS process and uninstalling the agent.
	Supported OSs: Linux.
	NOTE
	• Enabling the self-protection policy has the following impacts:
	  • The agent cannot be uninstalled using commands but can be uninstalled on the HSS console.
	  • HSS processes cannot be terminated.
		×	×	×	√	√	√

5 Provided Free of Charge

HSS provides the following free services:

- Free trial of HSS basic edition for 30 days

  When purchasing an ECS, you can select HSS basic edition for free for 30 days. The HSS basic edition can detect OS vulnerabilities, weak passwords, and brute-force attacks. For details, see **Features**. For more information, see **Free trial of HSS basic edition for 30 days**.

- Free health check

  HSS provides a free health check once a month for unprotected ECS and the Cloud Container Engine (CCE) that has enabled the free health check. HSS can detect software assets, OS vulnerabilities, and weak password risks of servers and generate security reports. For more information, see **Free health check**.

6 Personal Data Protection Mechanism

To ensure that your personal data, such as your username, password, and mobile phone number, will not be breached by unauthorized or unauthenticated entities or people, HSS encrypts your personnel data before storing it and control access to the data.

Personal Data

Table 6-1 describes the personal data generated or collected by HSS.

Table 6-1 Personal data

Type	Collection Method	Can Be Modified	Mandatory
Email	If 2FA is enabled, HSS periodically obtains from SMN the email addresses subscribing to notification topics.	No	Yes
Mobile phone number	If 2FA is enabled, HSS periodically obtains from SMN the mobile phone numbers subscribing to notification topics.	No	Yes
Login location	If HSS is enabled, it records user login locations.	No	Yes

Storage Mode

HSS uses encryption algorithms to encrypt users' sensitive data and stores encrypted data.

- Mobile phone number are encrypted before storage.
- Login locations are not sensitive data and stored in plaintext.

Access Control

User personal data is encrypted before being stored in the HSS database. The whitelist mechanism is used to control access to the database.

7 Security

7.1 Shared Responsibilities

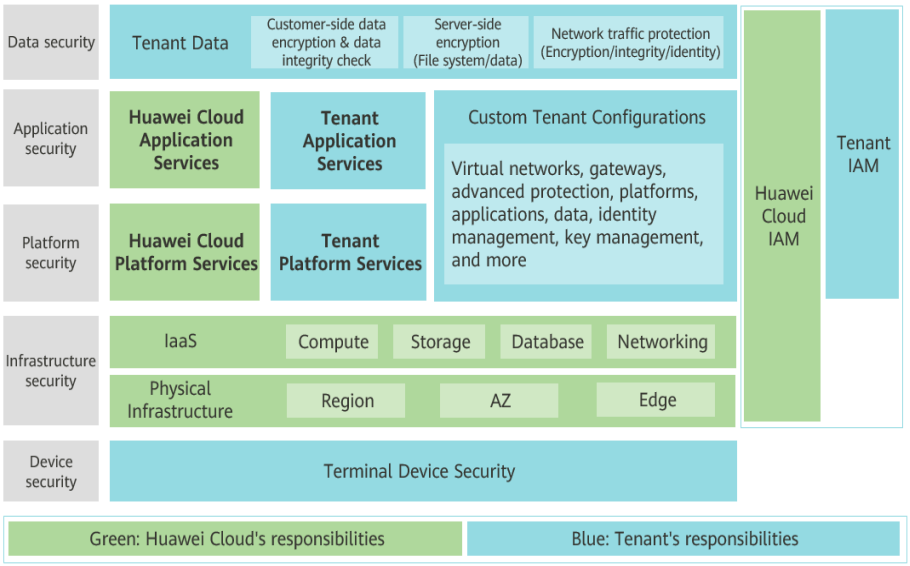
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Figure 7-1 illustrates the responsibilities shared by Huawei Cloud and users.

- **Huawei Cloud**: Ensure the security of cloud services and provide secure clouds. Huawei Cloud's security responsibilities include ensuring the security of our IaaS, PaaS, and SaaS services, as well as the physical environments of the Huawei Cloud data centers where our IaaS, PaaS, and SaaS services operate. Huawei Cloud is responsible for not only the security functions and performance of our infrastructure, cloud services, and technologies, but also for the overall cloud O&M security and, in the broader sense, the security and compliance of our infrastructure and services.
- **Tenant**: Use the cloud securely. Tenants of Huawei Cloud are responsible for the secure and effective management of the tenant-customized configurations of cloud services including IaaS, PaaS, and SaaS. This includes but is not limited to virtual networks, the OS of virtual machine hosts and guests, virtual firewalls, API Gateway, advanced security services, all types of cloud services, tenant data, identity accounts, and key management.

Huawei Cloud Security White Paper elaborates on the ideas and measures for building Huawei Cloud security, including cloud security strategies, the shared responsibility model, compliance and privacy, security organizations and personnel, infrastructure security, tenant service and security, engineering security, O&M security, and ecosystem security.

Figure 7-1 Huawei Cloud shared security responsibility model

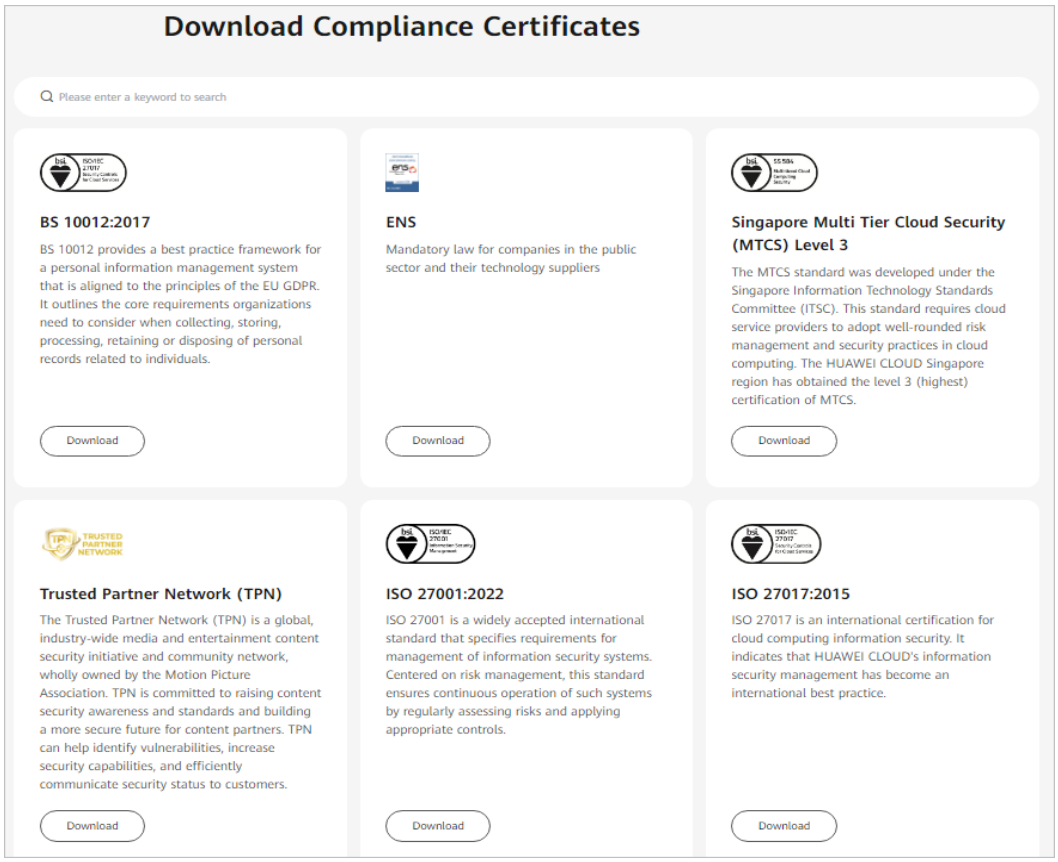


7.2 Certificates

Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International Organization for Standardization (ISO). You can **download** them from the console.

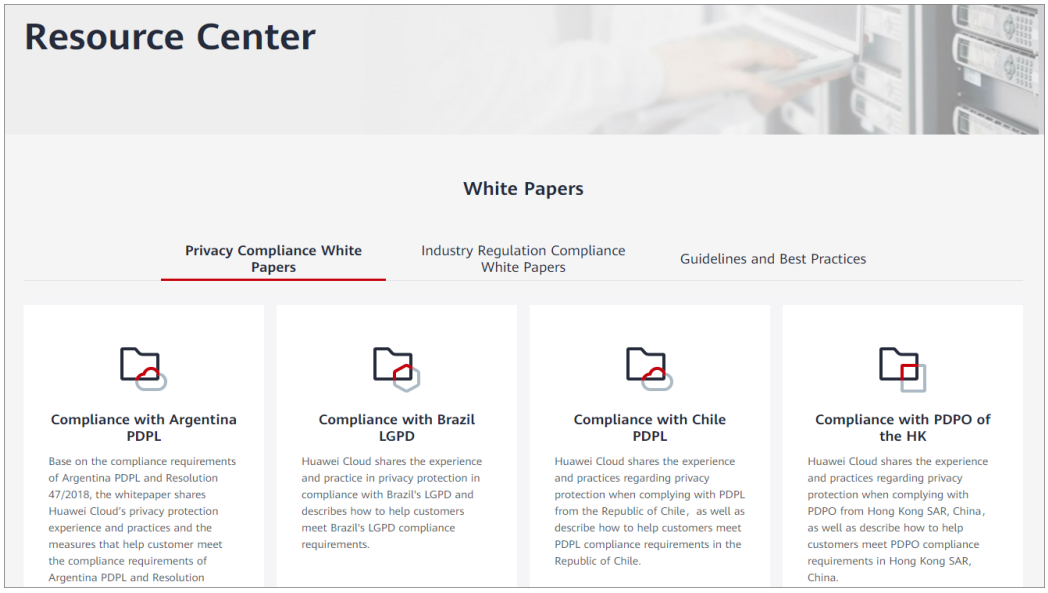
Figure 7-2 Downloading compliance certificates



Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see **Resource Center**.

Figure 7-3 Resource center



7.3 Asset Identification and Management

HSS collects 16 types of server and container asset information, including accounts, processes, open ports, auto-started items, software, web frameworks, and websites. It also displays the asset inventory, helping you find unsafe assets in servers and containers in a timely manner.

Table 7-1 HSS asset management functions

Function	Description	Reference
Asset overview	The asset overview displays the inventory of all server and container assets, including the agent status, quota status, accounts, ports, processes, software, and auto-started items. You can learn all asset statistics on a single page.	**Asset Overview**
Server fingerprints	HSS collects server accounts, open ports, processes, software, auto-started items, websites, web frameworks, middleware, kernel modules, web services, web applications, and database assets. It also displays asset details, helping you locate abnormal server assets.	**Server Fingerprints**
Container fingerprints	HSS collects container accounts, open ports, processes, software, auto-started items, websites, web frameworks, middleware, web services, web applications, databases, clusters, services, workloads, and instance assets. It also displays asset details, helping you find abnormal container assets.	**Container Fingerprints**

7.4 Identity Authentication and Access Control

Identity and Access Management (IAM) provides refined permissions management for HSS resources. You can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to HSS resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust a Huawei Cloud account or cloud service to perform professional and efficient O&M on your HSS resources.

  For details about HSS permission policies, see **Creating a User and Granting Permissions**.

7.5 Data Protection Technologies

HSS takes different measures to keep data stored in HSS secure and reliable.

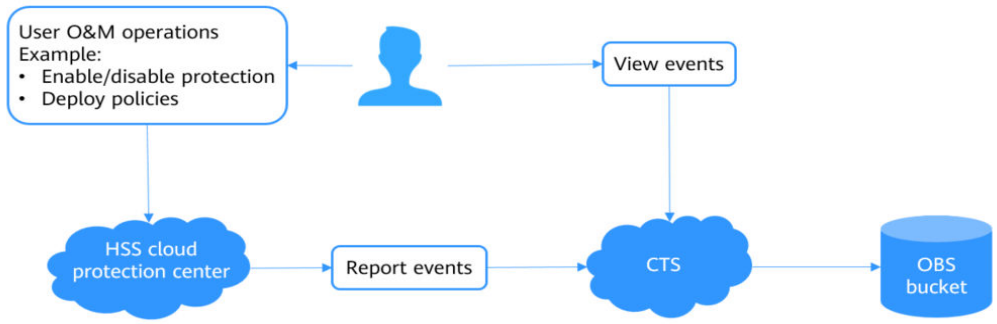
Measure	Description
Transmission encryption (HTTPS)	Data is encrypted when it is transmitted between microservices to prevent leakage or tampering during transmission. Your configurations are kept secure when transmitted over HTTPS.
Data redundancy	Data such as asset information and alarm events can be backed up and restored using copies.
Encrypted data storage	HSS encrypts sensitive data to prevent leakage.

You can also enable the Web Tamper Protection (WTP) edition protect business data.

For more information, see **Enabling the WTP Edition**.

7.6 Audit and Logging

Cloud Trace Service (CTS) keeps track of user activities and resource changes on your cloud resources. It helps you collect, store, and query operational records for security analysis, audit and compliance, and fault location.



For details about how to enable and configure CTS, see **Enabling CTS**.

For details about the HSS operations that can be audited by CTS, see **HSS Operations Supported by CTS**.

7.7 Service Resilience

HSS uses a four-level reliability architecture. It provides inspection, resistance, and recovery capabilities to help you manually or automatically recover services, enhancing data durability and reliability.

Table 7-2 Reliability architecture

Category	Capability	Description	Type
Inspection	Situation Awareness (SA)	HSS interconnects with SA and evaluates asset risks based on alarms, vulnerabilities, and baseline check results.	System
	Cloud Eye	With Cloud Eye, you can understand the resource usage and status of HSS, receive alarm notifications in a timely manner, and react to changes to keep your services run smoothly.	System
Resistance	Attack prevention	The agent provides self-protection, anti-removal, and anti-tamper capabilities.	Security
	Data backup	All key data can be backed up. Even if the database is completely damaged, services can be restored using the backup data.	System
	Service self-protection	HSS consists of microservices, which are independently deployed, started, and stopped. The agent strictly controls its resource usage. If its resource usage exceeds the threshold, the agent is isolated or a bypassing operation is performed to avoid affecting user workloads. If system resources are insufficient, the agent performance will be degraded.	System
Restoration	System restoration	A VM or service can be manually or automatically rebuilt if it is faulty.	System
	Process protection	If a process exits, the process will be automatically started to facilitate service recovery.	System

7.8 Risk Monitoring

Cloud Eye provides multi-dimensional monitoring for your resources on the cloud. It allows you to view the resource usage and service running status, and respond to exceptions in a timely manner to ensure smooth running of services.

HSS uses Cloud Eye to perform monitoring over resources and operations, helping you monitor server security and receive alarms and notifications in real time. You can check the number of unprotected servers, the number of unsafe servers, and the number of agents that are not installed or offline in real time.

For details about HSS metrics and how to create alarm rules, see **Monitoring**.

8 HSS Permissions Management

If you need to assign different permissions to employees in your enterprise to access your HSS resources, IAM is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you efficiently manage access to your cloud resources.

With IAM, you can use your Huawei Cloud account to create IAM users for your employees, and assign permissions to the users to control their access to specific resource types. For example, some software developers in your enterprise need to use HSS resources but must not delete them or perform any high-risk operations. To achieve this result, you can create IAM users for the software developers and grant them only the permissions required for using HSS resources.

If your Huawei Cloud account does not need individual IAM users for permissions management, then you may skip over this chapter.

IAM can be used free of charge. You pay only for the resources in your account. For more information about IAM, see **What Is IAM?**

HSS Permissions

By default, new IAM users do not have permissions assigned. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from their groups and can perform specified operations on cloud services.

HSS is a project-level service deployed and accessed in specific physical regions. To assign HSS permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When accessing HSS, the users need to switch to a region where they have been authorized to use cloud services.

You can grant permissions by using roles or policies.

- Roles: A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. This mechanism provides only a limited number of service-level roles for authorization. Some roles depend other roles to take effect. When you assign such roles to users, remember to assign the roles they depend on. However, roles are not an ideal choice for fine-grained authorization and secure access control.

- Policies: A type of fine-grained authorization that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and ideal for secure access control. For example, you can grant HSS users only the permissions for managing a certain type of resources. Most policies define permissions based on APIs.

The following table describes more details.

Table 8-1 System-defined permissions supported by HSS

Role/Policy Name	Description	Type	Dependency
HSS Administrator	HSS administrator, who has all permissions of HSS	System-defined role	• It depends on the **Tenant Guest** role. Tenant Guest: A global role, which must be assigned in the global project. • To purchase HSS protection quotas, you must have the **ECS ReadOnlyAccess**, **BSS Administrator**, and **TMS ReadOnlyAccess** roles. – **ECS ReadOnlyAccess**: read-only access permission for the ECS. This is a system policy. – **BSS Administrator**: a system role, which is the administrator of the billing center (BSS) and has full permissions for the service. – **TMS ReadOnlyAccess**: a system-defined policy that grants read-only access to TMS.
HSSFullAccess	All HSS permissions	Policy	To purchase HSS protection quotas, you must have the **BSS Administrator** role. **BSS Administrator**: a system role, which is the administrator of the billing center (BSS) and has full permissions for the service. **SMN ReadOnlyAccess**: a system-defined policy that grants read-only access to SMN.
HSSReadOnlyAccess	Read-only permission for HSS	Policy	**SMN ReadOnlyAccess**: a system-defined policy that grants read-only access to SMN.

Reference

- What Is IAM?
- Creating a User and Granting Permissions

9 Constraints and Limitations

Server Protection Restrictions

HSS can protect **Huawei Cloud servers, third-party cloud servers, and IDCs**. The following types of servers can be protected:

- Huawei Cloud
  - Huawei Cloud Elastic Cloud Server (ECS)
  - Huawei Cloud Bare Metal Server (BMS)
  - Workspace
- Third parties
  - Third-party cloud servers
  - On-premises IDCs

Container Protection Restrictions

HSS can protect **Huawei Cloud cluster containers, third-party cloud cluster containers, and on-premises IDC cluster containers**. For details about the supported container types, see **Table 9-1**.

Table 9-1 Container protection restrictions

Category	Supported Container Type	Constraints and Limitations
Huawei Cloud	• CCE cluster containers • Independent containers	• Supported **container runtime**: Docker and Containerd • Supported cluster editions: CCE standard and Turbo editions • Node resource requirements: at least 50 MiB memory and 200m CPU available • Resource usage restriction: When an agent is installed in a cluster, HSS creates an HSS namespace in the cluster.

Category	Supported Container Type	Constraints and Limitations
Third parties	• Alibaba Cloud cluster containers • Tencent Cloud cluster containers • Microsoft Cloud cluster containers • On-premises cluster containers • IDC on-premises cluster containers • Independent containers	• Supported cluster orchestration platforms: Kubernetes 1.19 or later • Supported node OS: Linux • Node specifications: at least 2 vCPUs, 4 GiB memory, 40 GiB system disk, and 100 GiB data disk • Clusters of Galera 3.34, MySQL 5.6.51, or earlier versions cannot be protected.

Protection Quota Limit

A server or container node can be protected by HSS only after a quota is allocated to it. Each server or container needs a quota.

The restrictions on the quotas are as follows:

- Quotas cannot be used across regions.

  Select a correct region during purchase. For details about how to select a region for different types of servers, see **the following table**.

  Table 9-2 Region restrictions on protection quotas

Category	Server	Region
Huawei Cloud	• ECS • BMS • Huawei Cloud Workspace	Regions where your ECSs/BMSs/Workspaces are deployed HSS cannot be used across regions. If the server and your protection quota are in different regions, **unsubscribe** from the quota and purchase a quota in the region where the server is deployed.

Category	Server	Region
Third parties	• Third-party cloud servers • On-premises IDCs	The region of quotas for third-party servers varies depending on the HSS access mode. • Internet access: The server can access HSS through the Internet. Currently, only certain regions allow servers to connect to HSS through the Internet. For details, see **In What Regions Is HSS Available to Non-Huawei Cloud Servers?** Select the region nearest to the region of the servers. • Direct Connect proxy access: The server cannot access the Internet and need to access HSS through Direct Connect and a proxy. This mode has no restrictions on regions. Select the region that you want to connect your servers to.

- A protection quota can be bound to only one server or container node.
- A maximum of 50,000 protection quotas can be purchased in a region.
- After a protection quota is purchased, your server or container is not protected yet. You need to go to the HSS console and install an agent for the server or container and enable protection as prompted.

OS Restrictions

Currently, the HSS agent and system vulnerability scan functions are not supported in certain OSs.

For details about the OS restrictions of HSS, see:

- **HSS restrictions on Windows (x86)**
- **HSS restrictions on Linux (x86)**
- **HSS restrictions on Linux (Arm)**

NOTE

- CentOS 6.x is no longer updated or maintained on the Linux official website, and HSS no longer supports CentOS 6.x or earlier.
- The meanings of the symbols in the table are as follows:
  - √: supported
  - ×: not supported

Table 9-3 HSS restrictions on Windows (x86)

OS	Agent	System Vulnerability Scan
Windows 10 (64-bit)	√ **NOTE** Only Huawei Cloud Workspace can use this OS.	×
Windows 11 (64-bit)	√ **NOTE** Only Huawei Cloud Workspace can use this OS.	×
Windows Server 2012 R2 Standard 64-bit English (40 GB)	√	√
Windows Server 2012 R2 Standard 64-bit Chinese (40 GB)	√	√
Windows Server 2012 R2 Datacenter 64-bit English (40 GB)	√	√
Windows Server 2012 R2 Datacenter 64-bit Chinese (40 GB)	√	√
Windows Server 2016 Standard 64-bit English (40 GB)	√	√
Windows Server 2016 Standard 64-bit Chinese (40 GB)	√	√
Windows Server 2016 Datacenter 64-bit English (40 GB)	√	√
Windows Server 2016 Datacenter 64-bit Chinese (40 GB)	√	√
Windows Server 2019 Datacenter 64-bit English (40 GB)	√	√
Windows Server 2019 Datacenter 64-bit Chinese (40 GB)	√	√
Windows Server 2022 Datacenter 64-bit English (40 GB)	√	×
Windows Server 2022 Datacenter 64-bit Chinese (40 GB)	√	×

Table 9-4 HSS restrictions on Linux (x86)

OS	Agent	System Vulnerability Scan
CentOS 7.4 (64-bit)	√	√
CentOS 7.5 (64-bit)	√	√
CentOS 7.6 (64-bit)	√	√
CentOS 7.7 (64-bit)	√	√
CentOS 7.8 (64-bit)	√	√
CentOS 7.9 (64-bit)	√	√
CentOS 8.1 (64-bit)	√	×
CentOS 8.2 (64-bit)	√	×
CentOS 8 (64-bit)	√	×
CentOS 9 (64-bit)	√	×
Debian 9 (64-bit)	√	√
Debian 10 (64-bit)	√	√
Debian 11.0.0 (64-bit)	√	√
Debian 11.1.0 (64-bit)	√	√
Debian 12.0.0 (64-bit)	√	×
EulerOS 2.2 (64-bit)	√	√
EulerOS 2.3 (64-bit)	√	√
EulerOS 2.5 (64-bit)	√	√
EulerOS 2.7 (64-bit)	√	×
EulerOS 2.9 (64-bit)	√	√
EulerOS 2.10 (64-bit)	√	√
EulerOS 2.11 (64-bit)	√	√
EulerOS 2.12 (64-bit)	√	√
Fedora 28 (64-bit)	√	×
Fedora 31 (64-bit)	√	×
Fedora 32 (64-bit)	√	×
Fedora 33 (64-bit)	√	×

OS	Agent	System Vulnerability Scan
Fedora 34 (64-bit)	√	×
Ubuntu 16.04 (64-bit)	√	√
Ubuntu 18.04 (64-bit)	√	√
Ubuntu 20.04 (64-bit)	√	√
Ubuntu 22.04 (64-bit)	√	√
Ubuntu 24.04 (64-bit)	√ **NOTE** Currently, brute-force attack detection is not supported.	×
Red Hat 7.4 (64-bit)	√	×
Red Hat 7.6 (64-bit)	√	×
Red Hat 8.0 (64-bit)	√	×
Red Hat 8.7 (64-bit)	√	×
OpenEuler 20.03 LTS (64-bit)	√	√
OpenEuler 20.03 LTS SP4 (64-bit)	√	×
OpenEuler 22.03 LTS SP3 (64-bit)	√	×
OpenEuler 22.03 LTS (64-bit)	√	×
OpenEuler 22.03 LTS SP4 (64-bit)	√	×
AlmaLinux 8.4 (64-bit)	√	√
AlmaLinux 9.0 (64-bit)	√	×
Rocky Linux 8.4 (64-bit)	√	×
Rocky Linux 8.5 (64-bit)	√	×

OS	Agent	System Vulnerability Scan
Rocky Linux 9.0 (64-bit)	√	×
HCE 1.1 (64-bit)	√	√
HCE 2.0 (64-bit)	√	√
SUSE 12 SP5 (64-bit)	√	√
SUSE 15 (64-bit)	√	×
SUSE 15 SP1 (64-bit)	√	√
SUSE 15 SP2 (64-bit)	√	√
SUSE 15 SP3 (64-bit)	√	×
SUSE 15.5 (64-bit)	√	×
SUSE 15 SP6 (64-bit)	√ **NOTE** Currently, brute-force attack detection is not supported.	×
Kylin V10 (64-bit)	√	√
Kylin V10 SP3 (64-bit)	√	×
UnionTech OS 1050u2e	√ **NOTE** Currently, file escape detection is not supported.	√

Table 9-5 HSS restrictions on Linux (Arm)

OS	Agent	System Vulnerability Scan
CentOS 7.4 (64-bit)	√	√
CentOS 7.5 (64-bit)	√	√
CentOS 7.6 (64-bit)	√	√
CentOS 7.7 (64-bit)	√	√
CentOS 7.8 (64-bit)	√	√
CentOS 7.9 (64-bit)	√	√
CentOS 8.0 (64-bit)	√	×
CentOS 8.1 (64-bit)	√	×

OS	Agent	System Vulnerability Scan
CentOS 8.2 (64-bit)	√	×
CentOS 9 (64-bit)	√	×
EulerOS 2.8 (64-bit)	√	√
EulerOS 2.9 (64-bit)	√	√
EulerOS 2.10 (64-bit)	√	√
EulerOS 2.11 (64-bit)	√	√
EulerOS 2.12 (64-bit)	√	√
Fedora 29 (64-bit)	√	×
Ubuntu 18.04 (64-bit)	√	×
Ubuntu 20.04 (64-bit)	√	√
Ubuntu 22.04 (64-bit)	√	√
Ubuntu 24.04 (64-bit)	√ **NOTE** Currently, brute-force attack detection is not supported.	×
Kylin V7 (64-bit)	√	×
Kylin V10 (64-bit)	√	√
Kylin V10 SP3 (64-bit)	√	×
HCE 2.0 (64-bit)	√	√
UnionTech OS V20 (64-bit)	√	√ **NOTE** Only UnionTech OS V20 server editions E and D support system vulnerability scan.
UnionTech OS V20 1050e (64-bit)	√	√
UnionTech OS V20 1060e (64-bit)	√	√
OpenEuler 22.03 LTS (64-bit)	√	×

Agent Restrictions

- If third-party security software, such as 360 Total Security, Tencent Manager, and McAfee, is installed on the server, uninstall the software before installing the HSS agent. If the third-party security software is incompatible with the HSS agent, the HSS protection functions will be affected.
- After the agent is installed on the server or container node, the agent may modify the following system files or configurations:
  - Linux system files:
    - /etc/hosts.deny
    - /etc/hosts.allow
    - /etc/rc.local
    - /etc/ssh/sshd_config
    - /etc/pam.d/sshd
    - /etc/docker/daemon.json
    - /etc/sysctl.conf
    - /sys/fs/cgroup/cpu/ (A subdirectory will be created for the HSS process in this directory.)
    - /sys/kernel/debug/tracing/instances (A CSA instance will be created in this directory.)
  - Linux system configurations: iptables rules
  - Windows system configurations:
    - Firewall rules
    - System login event audit policy and the configuration of login security layer and authentication mode
    - Windows Remote Management trusted server list

Restrictions on Brute-force Attack Defense

Authorize the Windows firewall when you enable protection for a Windows server. Do not disable the Windows firewall while you use HSS.

If the Windows firewall is disabled, HSS cannot block the source IP addresses of brute-force attacks. This problem may persist even if the Windows firewall is enabled after being disabled.

10 Related Services

You can use SMN to receive alarm notifications, IAM service to manage user permissions, and Cloud Trace Service (CTS) to audit user behaviors.

Elastic Cloud Server (ECS)/Bare Metal Server (BMS)

HSS agents can be installed on Huawei Cloud ECSs, BMSs, or third-party servers. You are advised to use Huawei Cloud servers for better and more reliable service experience.

- For details about ECS, see the **Elastic Cloud Server User Guide**.
- For details about BMS, see **Bare Metal Server User Guide**.

Cloud Container Engine (CCE)

CCE can rapidly build a highly reliable container cluster based on cloud servers and add nodes to the cluster for management. HSS can install Hostguard-agent on the nodes to protect the container applications deployed on them.

NOTE

CCE is a high-performance, high-reliability service through which enterprises can manage containerized applications. CCE supports native Kubernetes applications and tools, allowing you to easily set up a container runtime environment on the cloud. For more information, see the *Container Service User Guide*.

Software Repository for Container (SWR)

SWR provides easy, secure, and reliable management over container images throughout their lifecycles, facilitating the deployment of containerized services. For more information, see the *Software Repository for Container User Guide*. HSS scans for vulnerabilities and configurations in container images to help you detect the container environment that cannot be achieved by traditional security software.

Simple Message Notification (SMN)

SMN is an extensible, high-performance message processing service.

- To enable alarm notifications, you must configure SMN first.
- After the SMN is enabled, you will receive alarm notifications sent from HSS if your server is attacked or have high risks detected.
- On the **Alarm Notification** tab, you can configure **Daily Alarm Notification** and **Real-Time Alarm Notification** as required.

For details about SMN, see *Simple Message Notification User Guide*.

Identity and Access Management

IAM is a free identity management service that can implement refined HSS user permission isolation and control based on HSS user identities. It is the basic permission management service and can be used free of charge.

For details about IAM, see *Identity and Access Management User Guide*.

Cloud Trace Service (CTS)

CTS is a professional log audit service that records user operations in HSS. You can use the records for security analysis, compliance auditing, resource tracking, and fault locating. It is the basic log management service and can be used free of charge.

For details about CTS, see *Cloud Trace Service User Guide*.

11 Basic Concepts

Account Cracking

Account cracking refers to the intruder behavior of guessing or cracking the password of an account.

Baseline

A baseline specifies the minimum security configuration requirements that the OS and database configurations must meet in terms of account management, password policy configuration, authorization management, service management, configuration management, network configuration, and permission management. HSS provides the cloud security practice baseline, the DJCP MLPS compliance baseline, and the general security standard baseline detection to meet diverse security compliance requirements.

Weak Password

A weak password can be easily cracked.

Malicious Program

A malicious program, such as a web shell, Trojan, worm, or virus, is developed with attack or illegal remote control intents.

Malware covertly inlays code into another program to run intrusive or disruptive programs and damage the security and integrity of the data on an infected server. Malware includes viruses, Trojans, and worms, classified by their ways of transmission.

HSS reports both identified and suspicious malware.

Ransomware

Ransomware emerged with the Bitcoin economy. It is a Trojan that is disguised as a legitimate email attachment or bundled software and tricks you into opening or installing it. It can also arrive on your servers through website or server intrusion.

Ransomware often uses a range of algorithms to encrypt the victim's files and demand a ransom payment to get the decryption key. Digital currencies such as

Bitcoin are typically used for the ransoms, making tracing and prosecuting the attackers difficult.

Ransomware interrupts businesses and can cause serious economic losses. We need to know how it works and how we can prevent it.

Two-Factor Authentication

Two-factor authentication (2FA) refers to the authentication of user login by the combination of the user password and a verification code.

Web Tamper Protection

Web Tamper Protection (WTP) is an HSS edition that protects your files, such as web pages, documents, and images, in specific directories against tampering and sabotage from hackers and viruses.

Cluster

A cluster consists of one or more ECSs (also known as nodes) in the same subnet. It provides a computing resource pool for running containers.

Node

In CGS, each node corresponds to an ECS. Containers run on nodes.

Image

An image is a special file system. It provides not only programs, libraries, resources, configuration files but also some configuration parameters required for a running container. A Docker image does not contain any dynamic data, and its content remains unchanged after being built.

Container

A container is the instance of an image and can be created, started, stopped, deleted, and suspended.

Container Runtime

Container runtime, one of the most important components of Kubernetes, manages the lifecycle of images and containers. Kubelet interacts with a container runtime through the Container Runtime Interface (CRI) to manage images and containers.

Security Policy

A security policy indicates the security rule that must be followed for a running container. If a container violates a security policy, a container exception is displayed on the **Runtime Security** page of the CGS management console.

Project

Projects are used to group and isolate OpenStack resources, including computing, storage, and network resources. A project can be a department or a project team.

Multiple projects can be created for one account.

Protection Quota

To protect a server, bind it to an HSS quota.

The quotas of different HSS editions you purchased are displayed on the console.

Example:

- If you have purchased an HSS enterprise edition quota, you can bind it to a server.
- If you have purchased 10 HSS enterprise edition quotas, you can bind them to 10 servers.

