SecMaster

Service Overview

Issue 05

Date 2024-02-29

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.

Contents

1 What Is SecMaster?

SecMaster is a next-generation cloud native security operation platform. Based on years of cloud security experience of Huawei Cloud, it enables integrated and automatic security operations through cloud asset management, security posture management, security information and incident management, security orchestration and automatic response, cloud security overview, simplified cloud security configuration, configurable defense policies, and intelligent and fast threat detection and response.

Why SecMaster?

- One-click security compliance: Huawei's accumulated global security compliance experience enables one click generation of compliance reports, helping users quickly implement cloud service security/privacy protection compliance.
- Comprehensive awareness on one screen: Alert incidents of security services are collected, associated, sorted, and made available for retrieval, enabling security operation situations to be comprehensively evaluated and dynamically displayed on a large screen.
- Global analysis across the cloud: Based on hundreds of millions of threat indicators accumulated by Huawei Cloud every day, SecMaster enables associated analysis to locate security threats, eliminate invalid alerts, and identify potential advanced threats.
- Integrated global handling: The built-in alert processing playbooks enable minute-level automatic response to more than 99% security incidents.

For more information about the advantages of SecMaster, see **Product Advantages**.

2 Features and Functions

Based on cloud native security, SecMaster provides a comprehensive closed-loop security handling process that contains log collection, security governance, intelligent analysis, situation awareness, and orchestration response, helping you protect cloud security.

SecMaster provides **Security Overview**, **Workspace Management**, **Security Governance**, **Security Situation**, **Resource Manager**, **Risk Prevention**, **Security Response**, **Security Orchestration**, **Data Collection**, and **Data Integration**.

Security Overview

The **Security Overview** page gives you a comprehensive view of your asset security posture together with other linked cloud security services to collectively display security assessment findings.

Table 2-1 Functions

Function Module	Description
Security Score	SecMaster comes in different editions to evaluate and score your cloud asset security. You can quickly learn of unhandled risks and their threats to your assets. The lower the security score, the greater the overall asset security risk.
Security Monitoring	You can view how many threats, vulnerabilities, and compliance risks that are not handled and view details of them.
Your Security Score over Time	You can view your security scores for the last 7 days.

Workspace Management

Workspaces are top-level workbenches in SecMaster. A single workspace can be bound to common projects, enterprise projects, and regions for different application scenarios.

Table 2-2 Functions

Function Module	Description
Workspaces	• Workspace management: A single workspace can be bound to common projects and regions to support workspace operation modes in different scenarios. • Workspace agencies: – Workspace data hosting: All workspaces of a single account can be aggregated to a workspace for cross-account centralized security operations. – Workspace hosting: You can create agencies to let a user centrally view the asset risks, alerts, and incidents of multiple workspaces.

Security Governance

Security Governance provides you with a security governance template and compliance scanning service and converts the standard clauses in the security compliance pack into check items.

Table 2-3 Functions

Function Module	Description
Security Governance	• Compliance Pack Huawei's open security governance templates include original standards and regulation terms, check policies, compliance evaluation items, and improvement suggestions from Huawei experts, covering PCI DSS, ISO27701, ISO27001, privacy protection, and other regulations and standards. You can subscribe to and unsubscribe from security compliance packs and view the evaluation results. • Policy Check Security Governance periodically detects the compliance status of cloud assets through code-based scanning. You can view compliance risks on the dashboard, and obtain corresponding improvement suggestions from Huawei experts. • Compliance Evaluation Security Governance integrates regulatory clauses and standard requirements into compliance pack check items. You complete evaluation of your services using the compliance pack, and view evaluation results. You can also view historical results, upload and download evidence, and take actions based on Huawei experts' improvement suggestions. • Result Display Security Governance displays the evaluation results and compliance status on the dashboard, including the compliance rates of the compliance packs you subscribed to, and the compliance rate of each term the regulations and standards, each security, as well as the policy check results. **NOTE** Security Governance is available to limited users. To use this function, contact Huawei Cloud technical support.

Security Situation

You can view the security overview on the large screen in real time and periodically subscribe to security operation reports to know the core security indicators.

Table 2-4 Functions

Function Module		Description
Situation Overview	Security Score	SecMaster evaluates and scores your cloud asset security. You can quickly learn of unhandled risks and their threats to your assets. The lower the security score, the greater the overall asset security risk.
	Security Monitoring	You can view how many threats, vulnerabilities, and compliance risks that are not handled and view details of them.
	Your Security Score over Time	You can view your security scores for the last 7 days.
Large Screen		AI analyzes and classifies massive cloud security data and then displays security incidents in real time on a large screen. The large screen display gives you a simple, intuitive, bird's eye view of the security of your entire network clearly and efficiently.
Reports		You can generate analysis reports. In this way, you can learn about the security status of your assets in a timely manner.
Task Center		Displays the tasks to be processed in a centralized manner.

Resource Manager

SecMaster automatically discovers and manages all assets on and off the cloud and displays the real-time security status of your assets.

Table 2-5 Functions

Function Module	Description
Resource Manager	Synchronizes the security statistics of all resources and allows you to view the name, service, and security status of a resource, helping you quickly locate security risks.

Risk Prevention

Risk prevention provides baseline check and vulnerability management to help your cloud security configuration meet authoritative security standards, such as

DJCP, ISO, and PCI, as well as Huawei Cloud security best practice standards. You can learn about the global vulnerability distribution.

Function Module	Description
Baseline Inspection	SecMaster can scan cloud baseline configurations to find out unsafe settings, report alerts for incidents, and offer hardening suggestions to you.
Vulnerabilities	Automatically synchronizes vulnerability scanning result from Huawei Cloud Host Security Service (HSS), displays vulnerability scanning details by category, allows users to view vulnerability details, and provides vulnerability fixing suggestions.
Emergency Vulnerability Notices	SecMaster collects the latest information on known host security vulnerabilities every 5 minutes.
Policy Management	SecMaster supports centralized management of defense and emergency policies.

Security Response

Threat operation provides various threat detection models to help you detect threats from massive security logs and generate alerts; provides various security response playbooks to help you automatically analyze and handle alerts, and automatically harden security defense and security configurations.

Table 2-6 Functions

Function Module	Description
Incidents	Displays incident details in a centralized manner and supports manually or automatically turning alerts into incidents.
Alerts	Provides unified data class management (security operation objects) and built-in Huawei Cloud alert standards. Integrates and displays alerts of various cloud services, including HSS, WAF, and Anti-DDoS.
Indicators	Provides unified data class management (security operations objects) and built-in Huawei Cloud threat indicator standards. Integrates indicators of many cloud services and extracts indicators based on custom alert and incident rules.
Intelligent Modeling	Alert models can be built.

Function Module		Description
Security Analysis	Query and Analysis	• Search and analysis: Supports quick data search and analysis, quick filtering of security data for security survey, and quick locating of key data. • Statistics filtering: SecMaster supports quick analysis and statistics of data fields and quick data filtering based on the analysis result. Time series data supports statistics collection by default time partition, allowing data volume trend to be quickly spotted. SecMaster supports analysis, statistics, and sorting functions, and supports quick building of security analysis models. • Visualization: Visualized data analysis intuitively reflects service structure and trend, enabling customized analysis reports and analysis indicators to be easily created.
	Data Monitoring	Supports end-to-end data traffic monitoring and management.
	Data Consumption	• Provides streaming communication interfaces for data consumption and production, provides data pipelines that are integrated with SDKs, and allows customers to set policies for data production and consumption. • Provides Logstash open-source collection plug-ins for data consumption and production.

Security Orchestration

Security Orchestration supports playbook management, process management, data class management (security entity objects), and asset connection management. You can also customize playbooks and processes.

Security Orchestration allows you to flexibly orchestrate security response playbooks through drag-and-drop according to your service requirements. You can also flexibly extend and define security operation objects and interfaces.

Table 2-7 Functions

Function Module	Description
Objects	Manages operation objects such as data classes, data class types, and categorical mappings in a centralized manner.
Playbooks	Supports full lifecycle management of playbooks, processes, connections, and instances.

Function Module	Description
Layouts	Provides a visualized low-code development platform for customized layout of security analysis reports, alarm management, incident management, vulnerability management, baseline management, and threat indicator library management.
Plugins	Plug-ins used in the security orchestration process can be managed in a unified manner.

Data Collection

Collects various log data in multiple modes. After data is collected, historical data analysis and comparison, data association analysis, and unknown threat discovery can be quickly implemented.

Table 2-8 Functions

Function Module	Description
Data Collection	Logstash is used to collect various log data in multiple modes. After data is collected, historical data analysis and comparison, data association analysis, and unknown threat discovery can be quickly implemented.

Data Integration

Integrate security ecosystem products for associated operations or data interconnection. After the integration, you can search for and analyze all collected logs.

Table 2-9 Functions

Function Module	Description
Data Integration	The built-in log collection system supports one-click integration of logs from Huawei Cloud cloud products, covering storage, management, monitoring, and security. After the integration, you can search for and analyze all collected logs.

3 Product Advantages

Refined Indicators and Intuitive Situation Display

You can view the security overview on the large screen in real time and periodically subscribe to security operation reports to know the core security indicators.

Cloud Native Asset Stocktaking and Risk Prevention

All assets and security configurations on the cloud are automatically checked, and automatic hardening is provided to help you fix risky assets and insecure configurations. This avoids implicit channels and security device vulnerabilities introduced by traditional bolted-on security solutions.

Intelligent and Efficient Threat Detection, Response, and Handling

SecMaster focuses on finding true threats. By analyzing billions of security logs daily and leveraging the years of experience accumulated by the Huawei Cloud security operations team, SecMaster utilizes built-in models and analysis playbooks to reduce the interference from normal incidents. Threat and asset security profiling enables restoration of the entire attack chain. Risk handling playbooks can be configured for automatic response, simplifying operations and improving security and efficiency.

Environment Integration and Operational Collaboration for Ultimate Flexibility

You can connect to all security products, devices, and tools to connect data and operations (Bidirectional interconnection is supported). You can also define your own response models and analysis/handling playbooks to best meet your security requirements. You can use workspaces to enable large-scale organization collaboration and MSSP (Managed Security Service Provider) services.

4 Application Scenarios

The principle of cloud security is "30% R&D + 70% Operations". The "70% Operations" is where SecMaster is applied. The specific application scenarios of SecMaster are as follows:

Routine Security Operation

Inspect check items and implement the security operation process to achieve security objectives. Identify and mitigate risks, and continuously improve the process to prevent risk recurrence.

Key Incident Assurance

Provide 24/7 assurance during major festivals, holidays, activities, and conferences through attack defense to ensure service availability.

Security Drills

Provides security assurance in the attack defense drills organized by regulatory institutions through intrusion prevention, helping organizations pass the assessments in the drills.

Security Evaluation

Perform the white box baseline test, black box attack surface assessment, and attack vector detection before key incidents or drills to identify vulnerabilities.

5 Edition Differences

SecMaster provides three editions: basic, standard, and professional. Different editions have different features that apply to different scenarios. For details about feature differences, see **Feature Differences Between SecMaster Editions**. For details about features in each edition, see **Features and Functions**.

Editions

Table 5-1 describes SecMaster editions.

Table 5-1 SecMaster editions

Edition	Billing Mode	Description
Basic	Yearly/Monthly (Free)	Allows you to know your security situation.
Standard	Yearly/Monthly	• Provides the security situation information and DJCP compliance. • Provides plus features, such as **Large Screen**, **Intelligent Analysis**, and **Security Orchestration**.
Professional	• Pay-per-use billing • Yearly/Monthly billing	• Provides check on operation risks and regulation compliance. • Provides plus features, such as **Large Screen**, **Intelligent Analysis**, and **Security Orchestration**.

Feature Differences Between SecMaster Editions

The following table lists the function differences between SecMaster editions.

Table 5-2 Function differences between SecMaster editions

Function	Function Module	Description	Basic	Standard	Professional
Security Overview		Displays a comprehensive overview of asset security posture together with other linked cloud security services.	√	√	√
Workspace		• Workspace management: Workspaces are the root of SecMaster resources. A single workspace can be bound to general projects, enterprise projects, and regions for different application scenarios. • Workspace agencies: – Workspace data hosting: All workspaces of a single account can be aggregated to a workspace for cross-account centralized security operations. – Workspace hosting: You can create agencies to let a user centrally view the asset risks, alerts, and incidents of multiple workspaces.	√	√	√
Security Governance①		Security Governance provides you with security governance templates and checks your services against compliance policies that are built on the basis of the regulation terms in the security compliance packs.	√	√	√
Security Situation	Situation Overview	• Security Score: SecMaster scores security situation of your system, sorts out risks by severity, and display the risk defense capabilities of your system. • Security monitoring: displays security monitoring statistics in real time. • Your Security Score over Time: SecMaster displays your security scores for the last 7 days.	√	√	√
	Large Screen②	SecMaster displays the comprehensive security posture of your assets in the cloud in real time.	×	√	√

Function	Function Module	Description	Basic	Standard	Professional
	Security Report	You can generate analysis reports. In this way, you can learn about the security status of your assets in a timely manner.	×	×	√
	Task Hub	Displays the tasks to be processed in a centralized manner.	×	√	√
Asset Management		SecMaster synchronizes information about your resources and displays overall security posture in one place.	×	√	√
Risk Prevention	Baseline Inspection	SecMaster can scan cloud baseline configurations to find out unsafe settings, report alerts for incidents, and offer hardening suggestions to you.	×	√ (Supports basic baseline checks but does not provide details about check results.)	√
	Bug Management	Automatically synchronizes HSS vulnerability scanning result, displays vulnerability scanning details by category, and provides vulnerability fixing suggestions.	×	×	√
	Emergency Vulnerability Notice	SecMaster displays security vulnerabilities disclosed in the industry so that you can have a comprehensive understanding about your asset risks.	√	√	√
	Policy Management	SecMaster supports central management of defense and emergency policies.	×	√	√

Function	Function Module	Description	Basic	Standard	Professional
Threat Operations	Incident Management	Displays security threat incidents in a centralized manner.	×	√	√
	Alert Management	Provides unified security alert management and built-in Huawei Cloud alert standards. Integrates and displays alerts of other cloud services for centralized management.	×	√	√
	Indicators	Provides unified security threat indicator management and built-in Huawei Cloud threat indicator library standards. Security indicators from other cloud services can be accessed, and custom rules for extracting indicators are supported.	×	×	√
	Intelligent Modeling	Alert models can be built.	×	√	√
	Security Analysis②	Data can be queried, analyzed, consumed, monitored, and delivered.	×	√	√
Security Orchestration	Object Management	Manages data classes, data class types, and categorical mappings in a centralized manner.	×	√	√
	Playbooks②	Supports full lifecycle management of playbooks, processes, connections, and instances.	×	√	√
	Layout Management	Provides a visualized low-code development platform for customized layout of security analysis reports, alert management, incident management, vulnerability management, baseline management, and threat indicator library management.	×	√	√

Function	Function Module	Description	Basic	Standard	Professional
	Plug-in Management	Plug-ins used in the security orchestration process can be managed centrally.	×	×	√
Data Collection		Logstash is used to collect varied log data in multiple modes. After data is collected, historical data analysis and comparison, data association analysis, and unknown threat discovery can be quickly implemented.	×	√	√
Data Integration		Integrates security ecosystem products for associated operations or data interconnection. After the integration, you can search for and analyze all collected logs.	×	√ (Only cloud service alerts can be integrated.)	√
Directory Customization		You can view existing directories and change the layout.	×	√	√

NOTE
Symbol description:

- X: indicates that the function is unavailable in the corresponding edition.
- √: indicates that the function is available in the corresponding edition.
- ①: Security Governance is available to limited users. To use this function, contact Huawei Cloud technical support.
- ②: Some functions are supported in standard and professional editions, but you need to purchase a value-added package to use them, such as large screen, security analysis, and playbook orchestration.

6 Limitations and Constraints

The following table lists the limitations and constraints on using SecMaster.

Table 6-1 Limitations and constraints

Module	Constraints and Limitations
Billing	• The basic edition does not support the value-added packages. To use functions in the value-added packages, upgrade the basic edition to the standard or professional edition. • Value-added packages cannot be used independently. – To purchase a value-added package, purchase the standard or professional edition first. – If you unsubscribe from the pay-per-use professional edition, the system automatically unsubscribes from the value-added packages. – If you unsubscribe from the yearly/monthly standard or professional edition, you need to manually unsubscribe from the value-added packages you have.

Module	Constraints and Limitations
Workspaces	• Paid SecMaster: A maximum of five workspaces can be created for a single account in a single region. • Free SecMaster: Only one workspace can be created for a single account in a single region. • Permanent deletion of workspaces: Workspaces are deleted immediately and cannot be restored. • Workspace agencies: – A maximum of one workspace agency view can be created for an account in a region. – A maximum of 100 workspaces can be managed in a workspace agency view in a region for a single account or across several accounts. – A maximum of 10 workspaces can be managed in a workspace agency view under a single account in a region. – A maximum of 10 agencies can be created under a single account. • Currently, performing operations in different workspaces in multiple windows of the same browser is not supported.
Data Space/ Pipeline	• A maximum of five data spaces can be created in a workspace in a region for a single account. • A maximum of 20 pipelines can be created in a data space in a region for a single account.
Reports	A maximum of 10 security reports (including daily, weekly, and monthly reports) can be created in a single workspace of a single account.
Alert Models	• A maximum of 100 alert models can be created in a single workspace under a single account in a single region. • The running interval of an alert model must be greater than or equal to 5 minutes, and the time range for querying data must be less than or equal to 14 days.

Module	Constraints and Limitations
Query and Analysis	• A maximum of 500 results can be returned for a single analysis query. • A maximum of 50 shortcut queries can be created in a pipeline. That is, a maximum of 50 query analysis criteria can be saved as shortcut queries. • If there are over 50,000 results for a single query, the accuracy may decrease. In this case, you can select a short time range or apply more filter criteria to reduce the number of query results. • In aggregation queries (for example, GROUP BY statement) based on several fields, the default number of buckets for the second field is 10. If more than 10 buckets are generated, part of qualified data will be lost. In this case, the query results are not accurate.
Incidents, alerts, indicators, and vulnerabilities	• In a workspace of a single account, a maximum of 100 new alerts, incidents, indicators, or vulnerabilities can be added each day. • In a workspace of a single account, a maximum of 100 alerts can be converted into incidents each day.
Playbooks	• In a single workspace of an account, the scheduling frequency of a single playbook is greater than or equal to 5 minutes.
Playbook and Workflow Instances	The maximum number of retries within a day for a single workspace of a single account is as follows: • Manual retry: 100. After a retry, the playbook cannot be retried until the current execution is complete. • API retry: 100. After a retry, the playbook cannot be retried until the current execution is complete.
Classification & Mapping	• In a single workspace of a single account, a maximum of 50 classification & mapping templates can be created. • In a single workspace of a single account, the proportion of a classification to its mappings is 1:100. • A maximum of 100 classifications and mappings can be added to a workspace of a single account.

7 Security

7.1 Shared Responsibilities

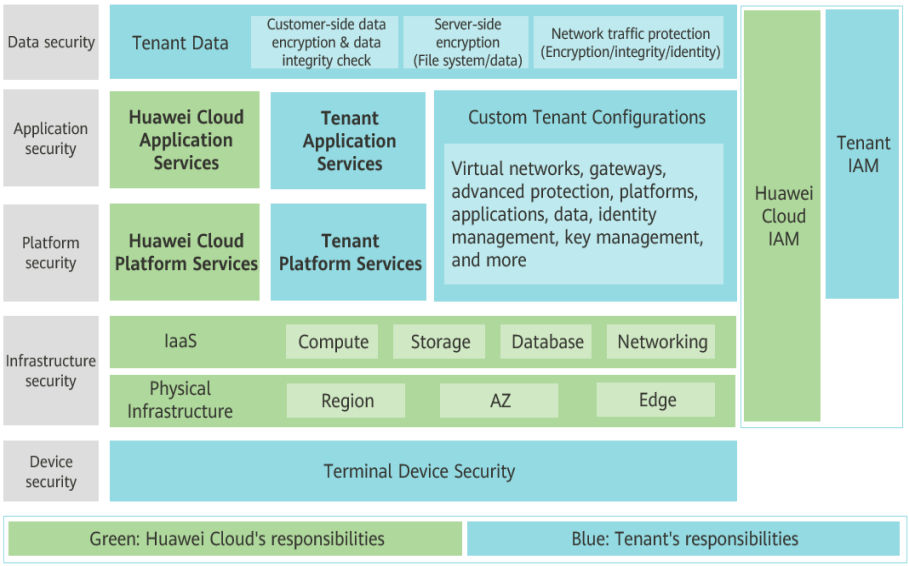
Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system 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 Identity Authentication and Access Control

SecMaster works with Identity and Access Management (IAM). SecMaster authenticates user identities and controls access to SecMaster through IAM.

Identity and Access Management (IAM) is a basic service of Huawei Cloud that provides permissions management to help you securely control access to SecMaster. With IAM, you can add users to a user group and configure policies to control their access to SecMaster resources. You can allow or deny access to a specific SecMaster resource in a fine-grained manner.

7.3 Data Protection Technologies

SecMaster takes different measures to keep data secure and reliable.

Table 7-1 SecMaster data protection methods and features

Method	Description
Static data protection	SecMaster encrypts sensitive data in your website traffic to keep the data from leakage.
Protection for data in transit	Data is encrypted when it is transmitted between microservices to prevent leakage or tampering during transmission. SecMaster keeps your configuration data secure as the configuration data is transmitted over HTTPS.

Method	Description
Data integrity verification	1. Data integrity is verified when SecMaster accesses cloud service alerts, vulnerabilities, and baselines. 2. When the SecMaster core data plane process is started, the configuration data enters the reliable mode to ensure data integrity (in scenarios such as network jitter, delay, and configuration data retransmission and retry).
Data isolation mechanism	SecMaster isolates its tenant zone from its management plane. Operation permissions for CFW are isolated by user. Your policies and logs are isolated from those of others.
Data destruction mechanism	To prevent information leakage caused by residual data, Huawei Cloud sets different retention periods based on the customer level. If the customer does not renew the subscription or recharge the account after the retention period expires, the data stored in the cloud service will be deleted and the cloud service resources will be released. SecMaster automatically detects cloud service subscription status and releases resources when the retention period expires.

In addition, SecMaster fully respects user privacy, complies with laws and regulations, and does not collect or store any user privacy data. For more privacy data usage and protection issues, see **Privacy Statement**.

7.4 Audit Logs

- Audit

  Cloud Trace Service (CTS) records operations on the cloud resources in your account. You can use the logs generated by CTS to perform security analysis, track resource changes, audit compliance, and locate faults.

  After you enable CTS and configure a tracker, CTS can record management and data traces of SecMaster for auditing.

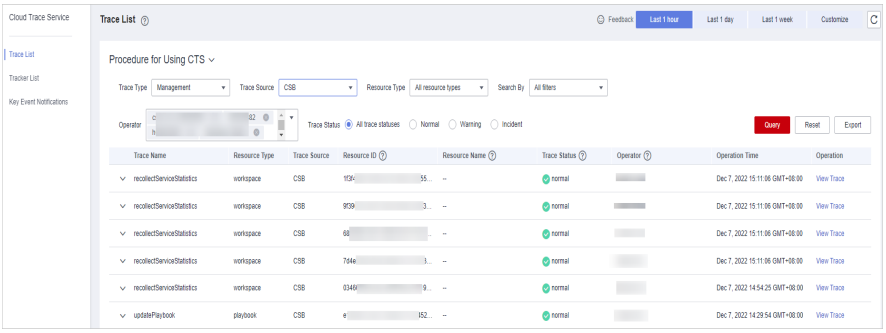
  For details about how to enable and configure CTS, see **Enabling CTS**.

- Logs
  - Querying logs

    After you enable CTS, the system starts recording operations on SecMaster. You can view the operation records of the last 7 days on the CTS console.

    Figure 7-2 shows how to view CTS logs.

Figure 7-2 Querying logs

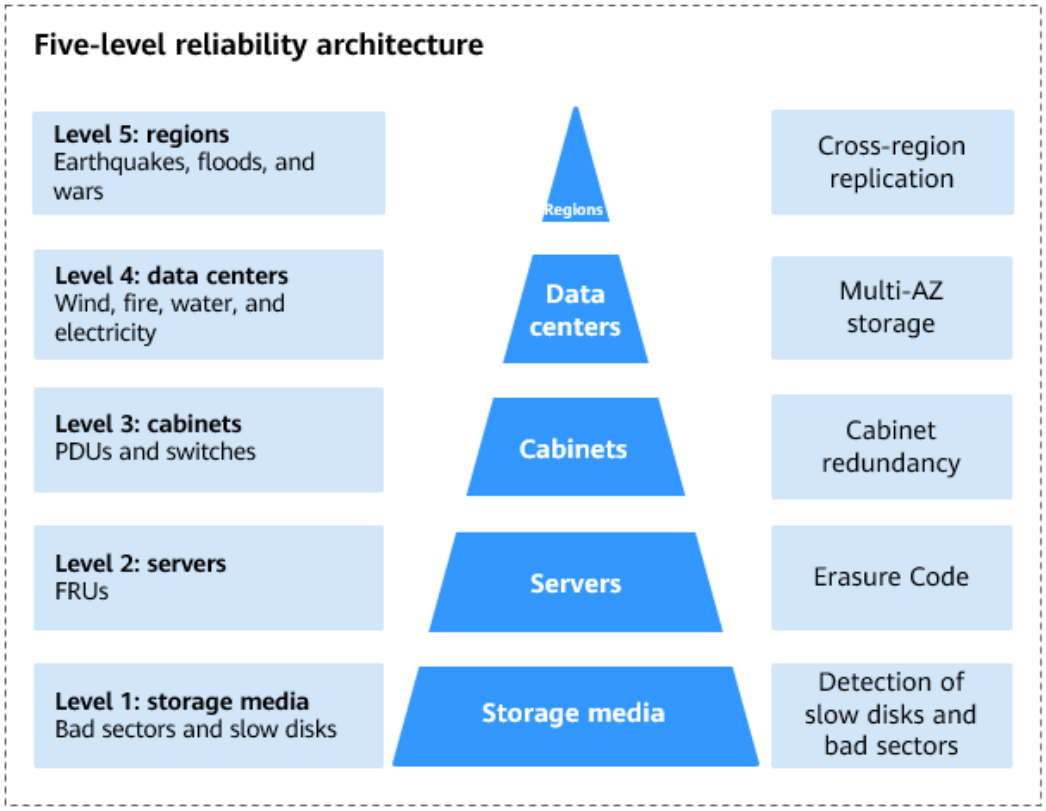


7.5 Service Resilience

Huawei Cloud SecMaster is mainly deployed in China. All deployed data centers are running properly. A data center serves as disaster recovery center for another. If a data center in city A is down, the data center in city B automatically takes over the job and serves your applications and data in compliance with the regulations to ensure service continuity. To minimize the service interruptions caused by hardware failures, natural disasters, or other disastrous incidents, Huawei Cloud SecMaster provides a DR plan.

SecMaster has high availability, fault tolerance, and scalability. If a fault occurs, the five-level reliability architecture of SecMaster supports different levels of reliability.

Currently, Huawei Cloud SecMaster is mainly deployed in China with many regions. All SecMaster components such as the management plane and engine are deployed as active/standby or cluster instances.



7.6 Risk Monitoring

SecMaster has interconnected with Cloud Eye (CES). You can view SecMaster running indicators on the CES management console. Cloud Eye is a multi-dimensional monitoring platform provided by Huawei Cloud for a wide range of cloud resources. With Cloud Eye, you can learn about the resource usage and service running status on the cloud, receive alerts in a timely manner, and respond quickly to exceptions to keep your cloud services stable.

As a cloud security operation platform, SecMaster can access security alerts of other cloud services and display alerts by alert type and level. SecMaster can accurately monitor threats and attacks on the cloud in real time and detect security alert incidents in your assets. You can define and schedule threat alert notifications to learn about threats and risks in a timely manner. The notification items you can define include threat list, alert type, and risk severity. This feature helps you learn about your security status in a timely manner.

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

Table 7-2 Risk monitoring

Incident Source	Incident	Alert Severity	Description	Handling Suggestion	Impact
SYS.SecMaster	Failed to create an exclusive engine.	Major	The underlying resources are insufficient.	Submit a service ticket to request adequate resources from the O&M personnel and try again.	Tn exclusive engine cannot be created.
SYS.SecMaster	The exclusive engine is not running properly.	Critical	The traffic is too heavy or there are malicious processes or plug-ins.	1. Check the executions of plug-ins and processes, see if they occupy too many resources. 2. Check the instance monitoring information to see whether there is a sharp instance increase.	The instance cannot be executed.
SYS.SecMaster	Failed to execute the playbook instance.	Minor	Playbooks or processes are wrongly configured.	Check the instance monitoring information to find the cause of the failure, and modify the playbook and process configuration.	None
SYS.SecMaster	The number of playbook instances increases sharply.	Minor	Playbooks or processes are wrongly configured.	Check the instance monitoring information to find the cause of the sharp increase, and modify the playbook and process configuration.	None
SYS.SecMaster	Log messages increase sharply.	Major	The upstream service suddenly generates a large number of logs.	Check whether the upstream service is normal.	None

Incident Source	Incident	Alert Severity	Description	Handling Suggestion	Impact
SYS.SecMaster	Log messages decrease sharply.	Major	Logs generated by the upstream service suddenly decrease.	Check whether upstream services are normal.	None

For details about monitoring alerts, see:

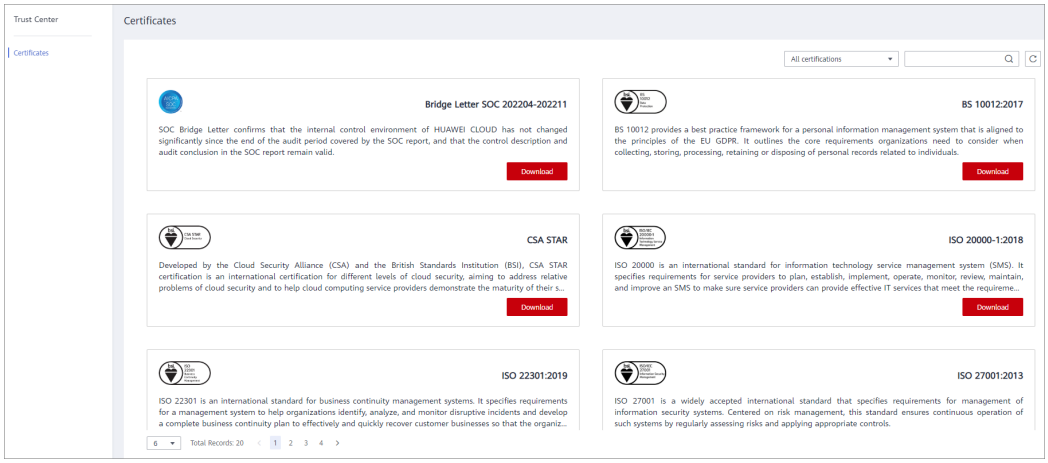
- **Vulnerability Management**
- **Cloud Service Baseline Overview**
- **Security Report**

7.7 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.

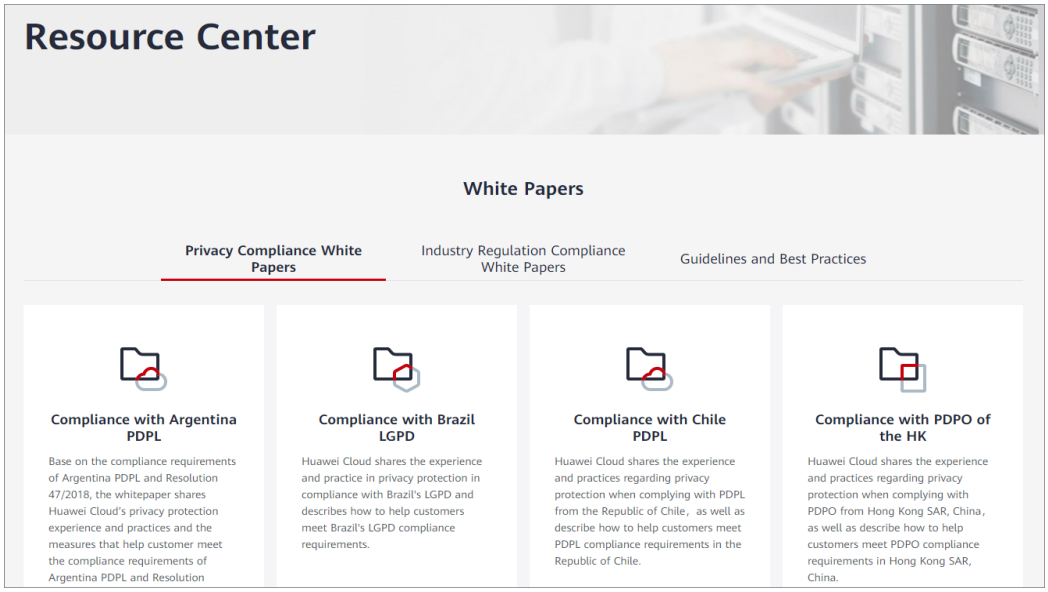
Figure 7-3 Downloading compliance certificates



Resource Center

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

Figure 7-4 Resource center



7.8 Security Orchestration

SecMaster Security Orchestration provides response playbooks for cloud security incidents. You can use playbooks to implement efficient and automatic response to security incidents. Its functions are as follows:

- Playbook management: you can use the built-in automatic response playbooks or customize playbooks.

  Orchestrating a playbook is to build the manual security operation process and software into a machine playbook.
- Workflow: Allows you to draw a playbook triggering flowchart.
- Asset Management: manages and displays key assets in a unified manner.
- Instance management: allows you to monitor and manage running instances and view records.
- Security Orchestration, Automation and Response (SOAR): You can orchestrate workflows to let SecMaster automatically handle security incidents and suspicious incidents.

For details about how to configure Security Orchestration, see **Security Orchestration**.

8 Permissions Management

If you want to assign different permissions to employees in your enterprise to access your SecMaster resources, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you securely manage access to your Huawei Cloud resources.

With IAM, you can create IAM users under your account for your employees, and assign permissions to the users to control their access to specific resource types. For example, you can use policies to grant different permissions to software developers in your enterprises to allow them to only use SecMaster but not perform certain high-risk operations, such as deletion of SecMaster data.

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

IAM is free. You pay only for the resources in your account. For more information about IAM, see **IAM Service Overview**.

SecMaster Permissions

By default, new IAM users do not have any permissions assigned. You can add a user to one or more groups to allow them to inherit the permissions from the groups to which they are added.

SecMaster is a project-level service deployed and accessed in specific physical regions. To assign 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. To access SecMaster, the users need to switch to a region where they have been authorized to use cloud services.

You can grant users permissions by using roles and policies.

- Roles: A type of coarse-grained authorization mechanism that defines permissions related to users responsibilities. Only a limited number of service-level roles for authorization are available. When using roles to grant permissions, you also need to assign dependency roles. Roles are not ideal for fine-grained authorization and secure access control.
- Policies: A type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under

certain conditions. This mechanism allows for more flexible policy-based authorization and meets secure access control requirements. For example, you can grant SecMaster users only the permissions for managing a certain type of resources.

Table 8-1 lists all SecMaster system permissions.

Table 8-1 System-defined permissions supported by SecMaster

Policy Name	Description	Type	Dependency
SecMaster FullAccess	All permissions of SecMaster.	System-defined policy	None
SecMaster ReadOnlyAccess	SecMaster read-only permission. Users granted with these permissions can only view SecMaster data but cannot configure SecMaster.	System-defined policy	None

SecMaster FullAccess Policy

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Action": [
                "secmaster:*:*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "vpc:vpcs:list",
                "vpc:subnets:get",
                "vpcep:endpoints:*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "obs:bucket:ListBucketVersions"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "iam:permissions:checkRoleForAgencyOnDomain",
                "iam:permissions:checkRoleForAgencyOnProject",
                "iam:permissions:checkRoleForAgency",
                "iam:permissions:grantRoleToAgency",
                "iam:permissions:grantRoleToAgencyOnDomain",
                "iam:permissions:grantRoleToAgencyOnProject",
                "iam:policies:*",
                "iam:agencies:*",
                "iam:roles:*",
                "iam:users:listUsers",
```



```
            "iam:tokens:assume"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "organizations:organizations:get",
            "organizations:delegatedAdministrators:list",
            "organizations:roots:list",
            "organizations:ous:list",
            "organizations:accounts:list"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "ecs:cloudServers:list"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "sts:agencies:assume"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "lts:log*:list*"
        ],
        "Effect": "Allow"
    }
  ]
}
```

SecMaster ReadOnlyAccess Policy

```
{
  "Version": "1.1",
  "Statement": [
    {
        "Action": [
            "secmaster:*:get*",
            "secmaster:*:list*"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "vpc:vpcs:list",
            "vpc:subnets:get",
            "vpcep:endpoints:get",
            "vpcep:endpoints:list"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "obs:bucket:ListBucketVersions"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "iam:permissions:checkRoleForAgencyOnDomain",
            "iam:permissions:checkRoleForAgencyOnProject",
            "iam:permissions:checkRoleForAgency",
            "iam:policies:get*",
            "iam:policies:list*",
```

```
            "iam:agencies:get*",
            "iam:agencies:list*",
            "iam:roles:get*",
            "iam:roles:list*",
            "iam:users:listUsers"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "organizations:organizations:get",
            "organizations:delegatedAdministrators:list",
            "organizations:roots:list",
            "organizations:ous:list",
            "organizations:accounts:list"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "ecs:cloudServers:list"
         ],
         "Effect": "Allow"
      },
      {
         "Action": [
            "lts:log*:list*"
         ],
         "Effect": "Allow"
      }
   ]
}
```

9 SecMaster and Other Services

This topic describes SecMaster and its linked services.

Security Services

SecMaster obtains necessary security incident records from security services such as **Host Security Service (HSS)**, **Web Application Firewall (WAF)**, and **Anti-DDoS**. SecMaster then uses big data mining and machine learning to intelligently analyze and identify attacks and intrusions, helping you understand the attack and intrusion processes. SecMaster also provides protective measures for you. For more details, see **What Are the Dependencies and Differences Between SecMaster and Other Security Services?**

Elastic Cloud Server (ECS)

SecMaster detects threats to your **ECSs** with linked service HSS, comprehensively displays ECS security risks, and provides protection suggestions.

Cloud Trace Service (CTS)

CTS generates traces to enable you to get a history of operations performed on SecMaster, allowing you to query, audit, and backtrack resource operation requests initiated from the management console as well as the responses to those requests.

CTS is used to record the operations you have performed on SecMaster for later querying, auditing, or backtracking.

Cloud Eye

Cloud Eye is a comprehensive platform to monitor a variety of cloud resources such as ECS and bandwidth usage. You can learn SecMaster indicators in a timely manner and respond to alerts in a timely manner to ensure smooth service running. For details, see the *Cloud Eye User Guide*.

TMS

Tag Management Service (TMS) is a visualization service that allows you to quickly and centrally manage tags, helping you manage workspace instances by tag.

Table 9-1 SecMaster operations supported by TMS

Operation	Resource Type	Incident Name
Querying the resource instance list	Workspace	listResourceInstance
Querying the number of resource instances	Workspace	countResourceInstance
Batch querying resource tags	Tag	batchTagResources
Batch deleting resource tags	Tag	batchUntagResources
Querying project tags	Tag	listProjectTag
Updating a tag value	Tag	updateTagValue
Querying resource tags	Tag	listResourceTag

Enterprise Management

You can manage multiple projects in an enterprise, separately settle their costs, and assign different personnel for them. A project can be started or stopped independently without affecting others. With **Enterprise Management**, you can easily manage your projects after creating an enterprise project for each of them.

SecMaster supports enterprise management. You can manage resources on SecMaster by enterprise project and set user permissions for each enterprise project.

10 Basic Concepts

This topic describes concepts used in SecMaster.

Security Risk

A security risk is a comprehensive evaluation of your assets, reflecting the security level of your assets within a period of time by a security score. A security score is for your reference to know the security situation of your assets.

Threat Alert

In general, threat alerts refer to threats that, due to natural, human, software, or hardware reasons, are detrimental to information systems or cause negative effects on the society. In SecMaster, threat alerts are detected security incidents that threaten asset security through big data technology.

Workspace

Workspaces are the root of SecMaster resources. A single workspace can be bound to general projects, enterprise projects, and regions for different application scenarios.

Data Space

A data space is a unit for data grouping, load balancing, and flow control. Data in the same data space shares the same load balancing policy.

Data Pipelines

A data transfer message topic and a storage index form a pipeline.

Classification and Mapping

Type matching and field mapping for cloud service alarms.

Security Orchestration

Security orchestration is a process that combines security capabilities (applications) and manual checks based on certain logical relationships to

complete a specific security operations procedure. Security functions of different security operations systems or components are encapsulated through programmable interfaces (APIs) during this process.

Security orchestration is a collaborative work mode that integrates various capabilities related to security operations, such as tools/technologies, workflows, and personnel.

Producer

A producer is a logical object used to construct data and transmit it to the server. It stores data in message queues.

Subscriber

A subscriber is used to subscribe to SecMaster pipeline messages. A pipeline can be subscribed to by multiple subscribers. SecMaster distributes messages through subscribers.

Consumer

A consumer is a running entity that receives and processes data. It consumes and processes messages in the SecMaster pipeline through subscribers.

Message Queue

A message queue is the container for data storage and transmission.

Threat Detection Model

A threat detection model is a trained AI recognition algorithm model. A threat detection model can automatically aggregate, analyze, and generate alerts for specific threats. This type of model has good generalization and anti-evasion capabilities. They can work in different service systems to defend against sophisticated emerging attacks.

A Change History

Released On	Description
2024-02-29	This issue is the fifth official release. • Updated the SecMaster policy content in **Permissions Management**. • Updated **Limitations and Constraints**: Added restrictions on workspaces and security analysis. • Optimized descriptions in **Features and Functions**.
2023-08-10	This issue is the fourth official release. • Updated **Features and Functions** and added policy management. • Updated **Edition Differences** and added policy management. • Moved the billing description section to the billing description manual.
2023-05-25	This issue is the third official release. • Added description of data collection in **Features and Functions**. • Updated the description in **Basic Concepts**.
2023-04-25	This issue is the second official release. • Updated the "Billing" Section and added descriptions of edition billing and upgrades. • Updated descriptions in **Edition Differences**.
2023-02-28	This issue is the first official release.

