ALIBABA CLOUD

Alibaba Cloud

Security Center

Product Introduction

Document Version: 20201019

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.What is Security Center?

Security Center is a centralized security management system that dynamically identifies and analyzes security threats, and generates alerts when threats are detected. It provides ransomware protection, antivirus protection, web tamper protection, and compliance assessments to ensure the security of cloud resources and on-premises servers. This allows you to automate security operations, responses, and threat tracing, and meet regulatory compliance requirements.

Security Center allows you to collect resource fingerprints and up to 10 types of security logs. It analyzes the security situation based on potential threats and delivers greater information traceability.

Security Center provides the following editions: Basic, Basic Anti-Virus, Advanced, and Enterprise. For more information, see Features. The following list provides an introduction to each edition:

- **Basic edition**

  The Basic edition offers basic **Security Enhancement** services free of charge. You can use the services to detect unusual logons to your servers, DDoS attacks, main types of vulnerabilities detected on servers, and service configuration risks. If you select **Security Enhancement** when you purchase an Elastic Compute Service (ECS) instance, the Basic edition of Security Center is automatically activated.

- **Basic Anti-Virus edition**

  The Basic Anti-Virus edition uses the subscription billing method. It provides security services, such as alerting and antivirus.

- **Advanced edition**

  The Advanced edition uses the subscription billing method. It provides security services, such as alerting, antivirus, vulnerability detection and fixing, and security reports.

- **Enterprise edition**

  The Enterprise edition uses the subscription billing method and provides a wide array of security features, including alerting, antivirus, vulnerability detection and fixing, baseline checks, asset fingerprints, and attack analysis.

Security Center complies with the standards of ISO 9001, ISO 20000, ISO 22301, ISO 27001, ISO 27017, ISO 27018, ISO 29151, ISO 27701, BS1 0012, CSA STAR, and PCI DSS.

2.Benefits

Security Center generates alerts when threats are detected. It also runs vulnerability and configuration baseline checks to reinforce system security and prevent attacks. To help you build a high-performance security system, Security Center supports security situation analysis and provides a graphical user interface to trace and analyze security events.

Security Center offers the following benefits:

- **Security event alerting and retrieval**

  Security Center monitors security events and provides solutions. To prevent intrusions, Security Center also analyzes and traces events that triggered alerts.

- **Vulnerability and baseline checks**

  Security Center automatically detects and lists vulnerabilities and configuration risks of your servers. It also provides solutions to fix vulnerabilities. This reinforces system security.

- **Risk quantification and prediction**

  Security Center supports quantified threat analysis and risk prediction based on machine learning.

- **Virus detection**

  Security Center can dynamically detect and remove viruses. Security Center supports data collection, masking, identification, and analysis. It also allows you to quarantine and restore files in the Security Center console. For more information, see Cloud threat detection.

- **International safety standards**

  Security Center complies with the standards of ISO 9001, ISO 20000, ISO 22301, ISO 27001, ISO 27017, ISO 27018, ISO 29151, ISO 27701, BS1 0012, CSA STAR, and PCI DSS.

3.Features

Security Center provides the Basic, Basic Anti-Virus, Advanced, and Enterprise editions. This topic describes the features supported by each edition.

- **Basic edition**

  The Basic edition offers basic **Security Enhancement** services free of charge. You can use the services to detect unusual logons to your servers, DDoS attacks, main types of vulnerabilities detected on servers, and service configuration risks. If you select **Security Enhancement** when you purchase an Elastic Compute Service (ECS) instance, the Basic edition of Security Center is automatically activated.

- **Basic Anti-Virus edition**

  The Basic Anti-Virus edition uses the subscription billing method. It provides security services, such as alerting and antivirus.

- **Advanced edition**

  The Advanced edition uses the subscription billing method. It provides security services, such as alerting, antivirus, vulnerability detection and fixing, and security reports.

- **Enterprise edition**

  The Enterprise edition uses the subscription billing method and provides a wide array of security features, including alerting, antivirus, vulnerability detection and fixing, baseline checks, asset fingerprints, and attack analysis.

> **Note** This section describes the symbols used in the following tables.
> - X: indicates that the feature is not supported by the edition.
> - √: indicates that the feature is supported by the edition.
> - Value-added: indicates a value-added service. If you want to use a value-added service, you must enable it when you purchase or upgrade Security Center.
> - Application required: indicates that the feature is available only after you apply for the feature and obtain the approval from Security Center.

Pricing comparison

Billing item		Basic	Basic Anti-Virus	Advanced	Enterprise
Basic fees		Free	USD 4.5 per asset per month	USD 9.5 per asset per month	USD 23.5 per asset per month
	Web Tamper Protection	Not supported	USD 142.6 per asset per month	USD 142.6 per asset per month	USD 142.6 per asset per month
	Anti-Ransomware	Not supported	USD 0.045 per GB per month	USD 0.045 per GB per month	USD 0.045 per GB per month

Billing item		Basic	Basic Anti-Virus	Advanced	Enterprise
Value-added service fees	Log Analysis	Not supported	USD 72.9 per TB per month	USD 72.9 per TB per month	USD 72.9 per TB per month
	Subscription duration		Unlimited	If the value of the Protected Servers parameter is greater than 10, monthly subscription is supported.	If the value of the Protected Servers parameter is greater than 10, monthly subscription is supported.

Billing item		Basic	Basic Anti-Virus	Advanced	Enterprise

Container security

Notice Security Center only performs security check for the container clusters or instances of the following Alibaba Cloud services:

- Container Service for Kubernetes: All Kubernetes clusters created by using templates support the security check feature.
- Container Registry: Only the Container Registry Enterprise edition supports the security check feature.

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Threat detection during container runtime	Security Center detects threats to Container Service for Kubernetes in real time, including viruses and malicious programs in the containers or on hosts, intrusion into the containers, and container escapes. It also generates alerts for these threats and warnings for high-risk operations.	X	X	X	√	Use Runtime Security to monitor ACK clusters and configure alerts
	Security Center detects the following items: • **Malicious image startups** Monitors open image sources in real time, such as Docker Hub, and generates alerts if an image that contains webshells or mining programs is installed on your server. • **Viruses and malicious programs** Detects viruses, trojans, mining programs, malicious scripts, and webshells in containers. • **Intrusion into containers** Detects intrusion into containers from application-layer attacks, unauthorized operations in containers, and application-to-application spread of malicious scripts in containers. • **Container escapes** Detects container escapes caused by improper container configurations, Docker vulnerabilities, or operating system vulnerabilities. • **High-risk operations** Detects sensitive host directories mounted to containers, Docker API leaks, Kubernetes API leaks, and containers started by suspicious privilege escalation. This minimizes the risk of attackers exploiting these vulnerabilities.	X	X	X	√	View and handle alert events

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Threat detection on Kubernetes containers	Security Center monitors the status of running containers in a Kubernetes cluster. This allows you to detect security risks and attacker intrusion in a timely manner. Security Center detects the following items: • Suspicious command execution on a Kubernetes API server • Mounting of suspicious directories to a pod • Transfer of Kubernetes service accounts from one application to another • Startup of a pod based on a malicious image	X	X	X	√	Threat detection for Kubernetes containers
Image signature	Security Center signs trusted container images and verifies the signatures to ensure that only trusted images are deployed. This prevents unauthorized container images from being started and improves asset security. Only Kubernetes clusters that are deployed in the China (Hong Kong) region support the image signature feature.	X	X	X	√	Container signature
Security check of container images	The image vulnerability detection feature is in public preview. Security Center detects vulnerabilities in container images to ensure that your images are secure and reliable. Note Security Center supports only the detection of container image vulnerabilities, but does not support automatic fixing of the detected vulnerabilities. If vulnerabilities are detected in a container image, we recommend that you follow the fixes and solutions provided by Security Center to manually reinforce image protection.	X	X	X	√	Image

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	security scans Documentation
Detection of application vulnerabilities in images	Security Center scans container-related middleware to detect application vulnerabilities in images. This ensures that images run in a secure environment.	X	X	X	√	
Detection of malicious image samples	Security Center provides image security scans to detect malicious image samples in your containers. This allows you to view the risks in your containers and reinforce the security of your assets.	X	X	X	√	
Container configuration security	Security Center performs security checks on the baseline configurations of containers. It also generates alerts based on the results of these checks. The security checks cover the following items: • **Alibaba Cloud Standard -DockerSecurity Baseline Check** Checks the baseline against the Alibaba Cloud standard of best practices for Docker. This check covers different dimensions, such as security audit, service configurations, and file permissions. Security Center generates alerts in a timely manner. • **Alibaba Cloud Standard - Kubernetes-Master security baseline check** Checks the baseline against the Alibaba Cloud standard of best practices for Kubernetes Master. • **Alibaba Cloud Standard - Kubernetes-Node security baseline check** Checks the baseline against the Alibaba Cloud standard of best practices for Kubernetes Node.	X	X	X	√	Overview

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Visualization of container security status	Security Center monitors the security status of containers in real time and displays it on the Assets page.	X	X	X	√	View the security information of containers

Security score

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Security score	Security Center displays a security score, which is calculated based on the security status of your assets, on the Overview page. A higher score indicates fewer risks in your assets.	√	√	√	√	• Security score • Improve the security score • Security score FAQ

Assets page

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Servers	Security Center displays security information about each protected server. The information includes the risk status, group, region, and VPC.	√	√	√	√	View the security status of a server
Containers	Security Center displays security information about each protected container group, container, and image. The information includes the risk status.	X	X	X	√	View the security information of containers
Websites	Security Center displays security information about each protected website. The information includes the root domain, subdomains, risk status, and alerts.	√	√	√	√	View website status
Cloud services	Security Center displays security information about each protected cloud service. The information includes the at-risk services and the type of each service, for example, Server Load Balancer (SLB), NAT Gateway, ApsaraDB for RDS, and ApsaraDB for MongoDB.	√	√	√	√	View the security status of cloud services

Virus defense

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Virus detection	The security experts of Security Center conduct automatic analysis on attack methods based on a large number of persistent virus samples. Alibaba Cloud developed the machine learning antivirus engine based on the attack analysis. You can detect and remove viruses with a few clicks.	X	√	√	√	

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Overview Documentation
Protection against viruses	Security Center quarantines major ransomware, DDoS trojans, mining programs and trojans, malicious programs, backdoor programs, and worms.	X	√	√	√	
Protection against ransomware	Security Center traps ransomware and supports data backup and restoration.	X	Value-added	Value-added	Value-added	Create a protection policy

Playbook

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Playbook	Security Center allows you to manage tasks. You can run tasks to enable automatic fixing of vulnerabilities in multiple assets at a time.	X	X	X	√	Playbook overview

Classified protection compliance check

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Classified protection compliance checks	Security Center checks whether your assets comply with classified protection regulations, including those on communication networks, region borders, computing environments, and management centers. It also generates compliance reports.	√	√	√	√	Classified protection compliance checks

Vulnerability fixing

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Linux software vulnerabilities	Security Center compares software versions by using the Open Vulnerability and Assessment Language (OVAL®) matching engine. It generates alerts if vulnerabilities recorded in the Common Vulnerabilities and Exposures (CVE) database are detected in the current version. Note The Basic edition only supports automatic vulnerability scans, but does not support vulnerability fixing or quick scan tasks. If you want to manually run quick scan tasks, you must upgrade Security Center to the Basic Anti-Virus, Advanced, or Enterprise edition. If you want Security Center to automatically fix detected vulnerabilities, you must upgrade Security Center to the Advanced or Enterprise edition.	√	√	√	√	Linux software vulnerabilities
	Vulnerability fixing: Security Center supports automatic fixing of system vulnerabilities and automatic creation of snapshots, which allow you to roll back to a specific snapshot to undo fixes.	X	X	√	√	

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Windows vulnerabilities	Security Center obtains Microsoft updates for Windows operating systems, detects high-risk vulnerabilities, and generates alerts for these vulnerabilities. Note The Basic edition only supports automatic vulnerability scans, but does not support vulnerability fixing or quick scan tasks. If you want to manually run quick scan tasks, you must upgrade Security Center to the Basic Anti-Virus, Advanced, or Enterprise edition. If you want Security Center to automatically fix detected vulnerabilities, you must upgrade Security Center to the Advanced or Enterprise edition.	√	√	√	√	Windows system vulnerabilities
	Vulnerability fixing: Security Center automatically identifies pre-patches for fixing vulnerabilities to prevent failures caused by a lack of the required pre-patches. This allows you to fix Windows vulnerabilities with a few clicks. Security Center also generates alerts for vulnerabilities that require a system restart after the vulnerabilities are fixed. This improves the efficiency of Windows vulnerability fixing.	X	X	√	√	
Web Content Management System (CMS) vulner	Security Center monitors web directories, recognizes common website builders, and checks the vulnerability database to identify vulnerabilities in website builders. Note The Basic edition only supports automatic vulnerability scans, but does not support vulnerability fixing or quick scan tasks. If you want to manually run quick scan tasks, you must upgrade Security Center to the Basic Anti-Virus, Advanced, or Enterprise edition. If you want Security Center to automatically fix detected vulnerabilities, you must upgrade Security Center to the Advanced or Enterprise edition.	√	√	√	√	Web-CMS vulnerabilities

abilities Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
	Vulnerability fixing: Security Center uses patches developed by Alibaba Cloud to replace and modify source code. This allows you to fix vulnerabilities with a few clicks.	X	X	√	√	
Emergency vulnerabilities	Security Center detects emergency vulnerabilities that are suddenly released to the public. Security Center does not support automatic fixing of emergency vulnerabilities. You must manually fix them by following instructions provided by Security Center.	√	√	√	√	Emergency vulnerability detection
Application vulnerabilities	Security Center detects weak passwords for system services and vulnerabilities in system services and applications. Note Only the Enterprise edition supports application vulnerability detection. If you want to detect application vulnerabilities in your assets, you must upgrade Security Center to the Enterprise edition.	X	X	X	√	Application vulnerabilities
Quick scan	Security Center allows you to manually run **quick scan** tasks on your assets to detect vulnerabilities in real time. Note Only the Enterprise edition supports application vulnerability detection. Therefore, only the Enterprise edition allows you to run **quick scan** tasks to detect application vulnerabilities. For more information about the types of vulnerabilities that can be detected by **quick scan** tasks in each edition, see Quick scan	√ (Only the detection of emergency vulnerabilities is supported.)	√ (The detection of application vulnerabilities is not supported.)	√ (The detection of application vulnerabilities is not supported.)	√	Quick scans

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Display of vulnerabilities that require immediate fixing	Security Center fixes emergency vulnerabilities and lists the vulnerabilities that require immediate fixing. This allows you to identify and fix vulnerabilities with high priorities.	X	X	√	√	Overview
YUM/APT source configuration	**YUM/APT Source Configuration** can be selected in the Settings pane of the Vulnerabilities page. This improves the success rate of vulnerability fixing.	X	X	√	√	Settings
Scan methods	**Real risk model** or **Full rule scan mode** can be selected as the scan mode in the Settings pane.	√	√	√	√	Settings

Baseline checks

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Baseline checks on servers	Security Center dispatches tasks to check server configurations and generates alerts if configuration risks are detected. Security Center allows you to specify check items, detection intervals, and servers to customize check policies. Custom check scripts are not supported. Security Center allows you to customize weak password rules. It checks the configurations of your cloud services by using a custom check policy and generates alerts if weak passwords are detected. Security Center performs baseline checks on the following items: • **High-risk vulnerabilities** Detects vulnerabilities in unauthorized operations in CouchDB or Docker. • **Containers** Detects risks on Docker, Kubernetes Master, and Kubernetes Node. • **Classified protection compliance** Performs security checks against classified protection level 3, classified protection level 2, and CIS standards. • **Best security practices** Performs security checks on Linux, Windows, and Redis. • **Weak passwords** Detects weak passwords during logons, such as ApsaraDB for MongoDB, FTP, and Linux logons.	X	X	√ (Only the detection of weak passwords is supported.)	√	Baseline checks
Baseline risk fixing	Security Center mitigates risks that are detected from the baseline checks of Alibaba Cloud security and classified protection compliance.	X	X	X	√	Manage baseline risks

Assessment of cloud service configurations

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Assessment of cloud service configurations	Security Center detects risks in the configurations of Alibaba Cloud services, such as ECS and ApsaraDB for RDS. Security Center performs detection on the following items: • **ECS** Checks whether the port access policies of security groups are too loose. • **SLB** Detects unnecessary ports that are accessible over the Internet. This type of port increases attack risks. • **RDS** Checks whether databases are accessible over the Internet and whether an access whitelist is configured. • **Actiontrail** Checks whether auditing of operations logs is enabled. This type of auditing facilitates event tracing. • **MFA** Checks whether two-factor authentication is enabled. This type of authentication protects Alibaba Cloud accounts. • **Other risks** Checks whether an SLB whitelist is configured and whether encrypted communications are enabled for ApsaraDB for RDS.	X	X	√	√	Overview

Security event alerts

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Suspicious processes	Security Center traces intrusion sources based on real attack-defense scenarios in the cloud, creates a process whitelist, and generates alerts if unauthorized processes or intrusion attacks are detected. Security Center builds nearly 1,000 process patterns for hundreds of processes and compares processes against these patterns to detect suspicious processes. Security Center detects the following items: • **Reverse shells** Detects suspicious command execution by Bash processes, and arbitrary command execution on servers under remote control. • **Suspicious command execution in databases** Detects suspicious command execution in databases, such as MySQL, PostgreSQL, SQL Server, Redis, and Oracle. • **Unauthorized operations in application processes** Detects unauthorized operations in application processes, such as Java, FTP, Tomcat, Docker container, and Lsass.exe processes. • **Unauthorized system processes** Detects unauthorized system processes, such as PowerShell, Secure Shell (SSH), Remote Desktop Protocol (RDP), SMBD, and Secure Copy Protocol (SCP) processes. • **Other suspicious processes** Detects other suspicious process activities, such as unusual access to Visual Basic Script (VBScript), unusual access to hosts, writing of crontab files, and webshell injection.	X	√	√	√	

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Webshells	Security Center supports detection of website script files, such as PHP, ASP, and JSP files, based on both servers and networks. Security Center performs the following detection: • **Server-based detection** Monitors network directory changes on servers in real time. • **Network-based detection** Captures webshell files and identifies network protocols to detect webshells.	X	√	√	√	
	Security Center also provides **webshell removal** to quarantine detected webshell files. You can restore quarantined files within 30 days.	X	√	√	√	
	Security Center provides basic detection services. Security Center detects the following items: • **Logons from disapproved locations** Detects logons from disapproved locations. Security Center automatically records locations where logons to ECS instances are allowed. These locations can also be manually added. If Security Center detects logons from disapproved locations, it generates alerts. • **Brute-force attacks** Detects logons to ECS instances after multiple failed attempts. In this case, the ECS instances may be under a brute-force attack.	√	√	√	√	

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Unusual logons	Security Center provides advanced detection services. Security Center detects the following items: • **Logons from disapproved IP addresses** Detects logons from disapproved IP addresses. Security Center allows you to specify approved IP addresses, such as the IP addresses of bastion hosts and private networks of companies, from which users are allowed to log on to ECS instances. If Security Center detects logons from disapproved IP addresses, it generates alerts. • **Logons from disapproved accounts** Detects logons from disapproved accounts. Security Center allows you to specify approved accounts, with which users are allowed to log on to ECS instances. If Security Center detects logons from disapproved accounts, it generates alerts. • **Logons during disapproved time periods** Detects logons during disapproved time periods. Security Center allows you to specify approved time periods, such as office hours, during which users are allowed to log on. If Security Center detects logons during disapproved time periods, it generates alerts.	X	X	√	√	

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Sensitive file tampering	Security Center monitors sensitive directories and files, and generates alerts if suspicious read, write, or delete operations are detected. Security Center detects the following items: • **System file tampering** Detects whether Bash and ps commands are replaced, or whether hidden and unauthorized processes are running. • **Removal of core website files** Detects malicious removal of core website files after servers are attacked. • **Trojan insertion** Detects whether malicious code is inserted into a website. If yes, trojans are automatically downloaded when users visit this website. • **Other suspicious activities** Detects whether ransomware tampers with the logon pages of Linux and MySQL, and inserts emails or Bitcoin wallet addresses.	X	√	√	√	Alerts

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Malicious processes	Security Server scans processes on a regular basis, monitors process startups, and detects viruses and trojans by using the cloud antivirus mechanism. You can terminate malicious processes and quarantine malicious files with a few clicks in the Security Server console. The virus library used for cloud antivirus has the following characteristics: • **Up-to-date virus data** The virus library is deployed, maintained, and updated by Alibaba Cloud in real time. This minimizes the risk of potential losses caused by outdated virus data. • **Diverse virus samples** All types of viruses are covered. Worldwide major antivirus engines are integrated. Sandboxes and machine learning engines that are developed by Alibaba Cloud are used. Security Center detects the following items: • **Ransomware** Detects file-encrypting ransomware, such as WannaCry and CryptoLocker. • **Attacks** Detects DDoS trojans, malicious scanning trojans, and spam trojans. • **Mining software** Detects resource-consuming software that uses servers for cryptocurrency mining. • **Zombies** Detects C&C trojans, malicious C&C connections, and attack tools. • **Other viruses** Detects worms, Mirai, and infectious viruses.	X	√	√	√	

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Suspicious network connections	Security Center monitors connections on servers and networks, and generates alerts if suspicious connections are detected. Security Center detects the following items: • **Suspicious connections to external IP addresses** Detects reverse shells and the Bash shell that establishes suspicious connections to external IP addresses. • **Attacks** Detects maliciously inserted software that is used to launch attacks, such as SYN floods, UDP floods, and ICMP floods. • **Suspicious communications** Detects suspicious webshell communications. • **Suspicious TCP packets** Detects scan activities that are initiated on your server and targets other devices.	X	√	√	√	
Other features	Security Center detects the following items: • Unusual disconnections of the Security Center agent • DDoS attacks	X	X	√	√	
Suspicious accounts	Security Center detects suspicious accounts that attempt to log on to your system based on user behavior analysis.	X	√	√	√	
Intrusion into applications	Security Center detects intrusion into applications, such as SQL Server.	X	√	√	√	
Threats to cloud services	Security Center detects unusual use of cloud services based on user behavior analysis. For example, an attacker uses your AccessKey pair to purchase a large number of ECS instances for mining.	X	√	√	√	

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Precise defense	Security Center automatically quarantines common Internet viruses, such as ransomware, DDoS trojans, mining and trojan programs, malicious programs, webshells, and computer worms. Alibaba Cloud security experts test and verify all of the automatically quarantined viruses to minimize false positive rates.	X	√	√	√	
Persistent webshells	Security Center detects persistent webshells on servers. After an attacker gains control over a server, the attacker typically places webshells, such as scripts, processes, and links, to persistently exploit the intrusion. Common persistent webshells include crontab jobs, automatic tasks, and system replacement files.	X	√	√	√	
Threats to web applications	Security Center detects intrusion activities that use web applications.	X	√	√	√	
Malicious scripts	Security Center detects malicious scripts on servers. Malicious scripts are classified into file-based scripts and fileless scripts. After an attacker gains control over a server, the attacker uses scripts for additional attacks. For example, the attacker may insert mining programs and webshells, and add administrator accounts. Languages of malicious scripts include Bash, Python, Perl, PowerShell, Batch, and VBScript.	X	√	√	√	
Threat intelligence	Security Center provides third-party threat intelligence sources.	X	Value-added	Value-added	Value-added	
Malicious network behavior	Security Center identifies unusual network behavior based on logs, such as communication content and host behavior logs. Malicious network behavior includes intrusion into hosts over open network services and unusual behavior of cracked hosts.	X	√	√	√	

Attack analysis

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Attack analysis	Security Center displays the details of web attacks and brute-force attacks on your server. It traces the attacker IP addresses and finds the flaws of the attacks.	X	X	X	√	Attack analysis

Detection of AccessKey pair leaks

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Detection of AccessKey pair leaks	Security Center monitors code hosting platforms, such as GitHub, to detect AccessKey pair leaks in source code that may be accidentally uploaded by company employees.	√	√	√	√	AccessKey leak detection

Log analysis

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Log analysis	Security Center supports retrieval and analysis of raw log data, including process startup events, external network connections, system logon events, five tuples, DNS queries, security logs, and alert logs. Note Only users of the Security Center Enterprise Edition can view network logs. Users of the Security Center Basic Anti-Virus or Advanced Edition cannot view network logs. On the Log Analysis page of the Security Center console, users of the Basic Anti-Virus or Advanced Edition can view only security and host logs.	X	Value-added	Value-added	Value-added	Log analysis

Investigation of asset fingerprints

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Asset fingerprints	Security Center collects the following server information in real time: • **Ports** Collects and displays port listening information to check open ports. • **Accounts** Collects information about server accounts and granted permissions, and checks privileged accounts to detect privilege escalation activities. • **Processes** Collects and displays process snapshots to check trusted processes and detect untrusted processes. • **Software** Checks software installation information, and locates affected assets when high-risk vulnerabilities occur. • **Scheduled tasks** Collects information about scheduled tasks of your assets. • **Middleware** Collects information about middleware of your assets.	X	X	X	√	Overview of asset fingerprints

Security reports

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Security reports	Security Center allows you to customize security reports. After you enable this feature, Security Center sends daily emails with security statistics to the specified recipients.	X	X	√	√	Security reports

Application marketplace

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Application whitelist	Security Center allows you to add applications that run on the servers that need high-level defense to an application whitelist. Security Center identifies applications as trusted, suspicious, or malicious based on the application whitelist to prevent unauthorized applications from running.	Application required	Application required	Application required	Application required	Application control
Web tamper proofing	Security Center monitors website directories and restores maliciously modified files or directories by using backups. It protects websites from malicious modification, trojans, hidden links, and insertion of violence or pornography content. Security Center allows you to add trusted Windows and Linux processes to whitelists. After a process is added to a whitelist, Security Center no longer blocks the process.	X	Value-added	Value-added	Value-added	Web tamper proofing

Multi-account control

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Multi-account control	Security Center allows you to manage multiple Alibaba Cloud accounts and resource accounts. You can monitor the security status of accounts under a resource directory.	X	X	X	√	Multi-account control

Settings

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Settings	Proactive defense Automatically blocks common viruses, malicious network connections, and webshells connections, and uses bait to capture ransomware. You can enable or disable the following features: • Antivirus • Anti-ransomware (bait capture) • Webshell protection • Malicious behavior prevention	X	√	√	√	The anti-virus feature
	Webshell detection Periodically scans Web directories to detect webshells and trojans on servers.	X	√	√	√	Webshell detection
	Kubernetes threat detection Security Center monitors the status of running containers in a Kubernetes cluster. This allows you to detect security risks and attacker intrusion in a timely manner.	X	X	X	√	Threat detection for Kubernetes containers
	Security control Security control allows you to configure the IP address whitelist. Requests initiated from IP addresses in the whitelist are directly forwarded to destination servers. This prevents normal network traffic from being blocked.	√	√	√	√	Security control
	Access control Resource Access Management (RAM) allows you to create and manage RAM users, such as individuals, system administrators, and application administrators. You can manage RAM user permissions to control access to Alibaba Cloud resources.	√	√	√	√	Access control

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
	Protection modes Security Center provides multiple modes to protect your server in different scenarios. You can set the following protection modes to protect your server: • Basic protection mode. All editions support this mode. • High-security prevention mode. Only the Basic Anti-Virus, Advanced, and Enterprise editions support this mode. • Safeguard mode for major activities. Only the Enterprise edition supports this mode.	√	√	√	√	Manage protection modes
	Client protection After you enable the client protection feature, Security Center automatically intercepts unauthorized agent uninstallation. This feature prevents the agent from being uninstalled by attackers or terminated by other software.	√	√	√	√	Client protection
Notifications	Security Center allows you to customize alert notifications, such as specifying notification methods and alert severities. It sends the alert notifications by using text messages, emails, internal messages, or messages from DingTalk chatbots. You can configure notifications for the following items: • Vulnerabilities • Baseline checks • Security alerts • Information about AccessKey pair leak • Cloud service checks • Intelligence of emergency vulnerabilities • Web tamper proofing Note If you want to receive the alert notifications by using messages from DingTalk chatbots, you must upgrade Security Center to the Enterprise edition.	√	√	√	√	Notifications

Feature	Description	Basic edition	Basic Anti-Virus edition	Advanced edition	Enterprise edition	Documentation
Installation and uninstallation of the Security Center agent	Security Center allows you to install and uninstall the Security Center agent.	√	√	√	√	Install or uninstall the Security Center agent

Threat detection limits

When Security Center detects risks, it sends security alerts to you without delay. You can manage security alerts, scan for vulnerabilities, analyze attacks, and perform configuration assessment in the Security Center console. Security Center can also analyze alerts and automatically trace attacks. This reinforces the security of your assets. To protect your assets against attacks, we recommend that you regularly install the latest security patches on your server, and use other security services along with Security Center, such as Cloud Firewall and Web Application Firewall (WAF).

> **Note** Due to the evolution of attacks and viruses, and the variation of workload environments, security breaches may occur. We recommend that you use the alerting, vulnerability detection, baseline check, and configuration assessment features provided by Security Center to protect your assets against attacks.

4.Scenarios

Security Center can be used in the following scenarios:

- Real-time monitoring of business security in the cloud.

  Security Center can generate alarms for security events such as unusual logons, webshell injections, and malware.

- Periodic vulnerability detection and baseline check for cloud services.

  Security Center provides vulnerability detection, warns you of unsafe configurations, and odders fixes.

- Query and analysis of network logs, server logs, and user visits.
- Real-time monitoring of open ports on ECS instances and security issues, including AccessKey leaks, network intrusions, DDoS attacks, and bots.
- Tracking of intrusions, such as webshell injections, malware, and ransomware in ECS, to analyze the patterns of intrusions and locate the causes.
- Review the related events on the same page, and make you easier to analyze and handle the events and alerts.
- Customize the rules of alerts based on your business requirements.

5.Limits

This topic describes the limits of Security Center.

Threat detection limits

When Security Center detects risks, it sends security alerts to you without delay. You can process security alerts, scan for vulnerabilities, analyze attacks, and check security settings in the Security Center console. Security Center can analyze alerts and automatically trace attacks. This helps you protect your assets. Security Center supports a wide array of protection features. We recommend that you also install the latest system patches on your server, and use multiple security services, such as Cloud Firewall and Web Application Firewall (WAF), to better protect your assets against attacks.

> **Note** Due to the rapid adaption of attacks, viruses, and the variation of the workload environments, security breaches may occur. We recommend that you use the alerting, vulnerability detection, baseline check, and configuration assessment features provided by Security Center to better protect your assets against attacks.

Logstore limits

All logs of Security Center are stored in dedicated Logstores.

- You cannot use the Log Service API or SDK to import data into the dedicated Logstores or modify the attributes of the dedicated Logstores, such as the retention period.
- Dedicated Logstores have no limits on queries, statistics, alerts, and streaming data consumption.
- Dedicated Logstores do not incur charges on the condition that Log Service does not have overdue payments.
- The default reports may be updated in later versions.

6.Information collection scope

After the Security Center agent is installed on your servers, it collaborates with Alibaba Cloud to protect your servers. Security Center provides a wide array of features, including security alerts, vulnerability management, antivirus, baseline checks, and attack analysis.

This topic describes the information that can be collected by Security Center.

> **Note** Changes in the following information will be posted on the Alibaba Cloud international site. If you do not accept the changes, you can stop using Alibaba Cloud Security Center. In this case, you can uninstall the agent from your servers. For more information, see Uninstall the Security Center agent. If you continue using Alibaba Cloud Security Center, you are deemed to have accepted these changes.

Suspicious files

Security Center detects suspicious files on your servers. After a suspicious file is detected by Security Center, information about the file is uploaded to Alibaba Cloud for further verification. The file information includes but is not limited to the file path, MD5 hash value, and creation time. If the suspicious file is determined as a malicious file, Security Center sends you an alert.

Suspicious processes

Security Center detects suspicious processes on your servers. After a suspicious process is detected by Security Center, information about the process is uploaded to Alibaba Cloud for further verification. The process information includes but is not limited to the process name, parameters used to start the process, file path of the process, and start time of the process. If the suspicious process is determined as a malicious process, Security Center sends you an alert.

Accounts

Security Center provides features such as logon audit, suspicious account alerting, and brute-force attack prevention. Security Center regularly analyzes and uploads account and logon information about protected servers. The account information includes but is not limited to the usernames and user permissions. The logon information includes but is not limited to the usernames and IP addresses that are used for logons. If the logon is determined as an usual logon, Security Center sends you an alert.

Suspicious connections

Security Center detects suspicious network connections to your servers. After a suspicious network connection is detected by Security Center, information about the connection is uploaded to Alibaba Cloud for further verification. The connection information includes but is not limited to the source IP address, source port, destination IP address, and destination port. If the suspicious network connection is determined as malicious, Security Center sends you an alert.

Server assets

Security Center supports server asset management. Security Center regularly collects information about servers, including but not limited to the software information, port listening information, and information about the websites running on your servers. You can log on to the Security Center console and view the information on the **Assets** page.

Container image security

Security Center scans container images. Security Center regularly scans containers to detect whether vulnerabilities and malicious files exist. You can log on to the Security Center console, choose **Image Security**, and view detected vulnerabilities and malicious files.

Container security during runtime

To ensure container security during runtime, Security Center dynamically detects threats, including viruses, malicious programs, intrusions, container escapes, and high-risk operations in running containers. If risks are detected during container runtime, Security Center sends you an alert.

7.FAQ

This topic provides answers to some commonly asked questions about the purchase of Security Center.

I have tried the Enterprise edition of Security Center free of charge. Can I reapply for the free trial?

No, you cannot reapply for the free trial.

Each Alibaba Cloud account is limited to one free trial for the Security Center Enterprise Edition.

How do I apply for a 7-day free trial of the Security Center Enterprise edition?

Before you apply for the 7-day free trial, make sure that the following conditions are met:

- Security Center Basic is activated for your Alibaba Cloud account.

  You have not purchased one of the following editions of Security Center: Basic Anti-virus, Advanced, and Enterprise. By default, all Alibaba Cloud accounts can use Security Center Basic.

  > **Note** Assume that you have purchased Security Center Basic Anti-Virus, Advanced, or Enterprise before, but the service has expired and you have not renewed it. In this case, Security Center is automatically downgraded to the Basic edition.

- You have not applied for a seven-day free trial of Security Center Enterprise before.
- At least one Elastic Compute Service (ECS) instance is purchased.

After you confirm that the conditions are met, perform the following operations to apply for the 7-day free trial:

1. Go to the Security Center product page.

2. Click **Free Trial** and log on to the Security Center console by using your Alibaba Cloud account.
3. In the **7-Day Free Trial** dialog box, click **Free Trial of Enterprise Edition**.

> **Note** Each Alibaba Cloud account is limited to one free trial for the Security Center Enterprise Edition.

Can I purchase Security Center on a monthly basis?

Yes, you can purchase and renew Security Center on a monthly basis. The minimum subscription duration that you can purchase varies based on the number of servers that you want to protect.

- If the number is in the range of 2 to 10, the minimum subscription duration is six months.
- If the number is greater than 10, the minimum subscription duration is one month.

> **Note** If the number is 1, the minimum subscription duration is one year.

For more information about the pricing of Security Center, see Billing methods.

Are there differences between each edition of Security Center?

Yes, Security Center provides the Basic, Basic Anti-Virus, Advanced, and Enterprise editions, which differ from each other.

- **Basic edition**

  The Basic edition offers basic **Security Enhancement** services free of charge. You can use the services to detect unusual logons to your servers, DDoS attacks, main types of vulnerabilities detected on servers, and service configuration risks. If you select **Security Enhancement** when you purchase an Elastic Compute Service (ECS) instance, the Basic edition of Security Center is automatically activated.

- **Basic Anti-Virus edition**

  The Basic Anti-Virus edition uses the subscription billing method. It provides security services, such as alerting and antivirus.

- **Advanced edition**

  The Advanced edition uses the subscription billing method. It provides security services, such as alerting, antivirus, vulnerability detection and fixing, and security reports.

- **Enterprise edition**

  The Enterprise edition uses the subscription billing method and provides a wide array of security features, including alerting, antivirus, vulnerability detection and fixing, baseline checks, asset fingerprints, and attack analysis.

The Basic Anti-Virus edition is priced asUSD 4.5 per month. Why is the price on the buy page higher thanUSD 4.5?

The price on the buy page is based on the following two factors:

- Protected Servers

The Protected Servers parameter specifies the total number of assets protected by Security Center. The assets include Alibaba Cloud Elastic Compute Service (ECS) instances and external servers that have the Security Center agent installed. The default value is the total number of ECS instances and external servers that have the Security Center agent installed under your Alibaba Cloud account. If the number of protected server is greater than 1, the price on the buy page is higher thanUSD 4.5 per month.

- Enabled value-added services

  Security Center provides value-added services, such as web tamper proofing, log analysis, and anti-ransomware. When you purchase Security Center, the default values of the Log Storage Capacity and Anti-ransomware parameters are used. If you do not need log analysis and anti-ransomware, set the Log Storage Capacity and Anti-ransomware parameters to 0 GB.

I do not have an Alibaba Cloud ECS instance. Can I use Security Center to protect servers in on-premises data centers?

Yes, Security Center can protect Alibaba Cloud ECS instances, servers in on-premises data centers, and third-party cloud servers. Security Center can protect servers that have the Security Center agent installed. For more information, see Install the Security Center agent and Use Security Center to protect servers in on-premises data centers.

Can Security Center protect third-party cloud servers?

Yes, Security Center can protect servers from third-party providers, such as Amazon Web Services (AWS), Tencent Cloud, QingCloud, and UCloud. Security Center can protect servers that have the Security Center agent installed. For more information, see Install the Security Center agent on servers that are not deployed on Alibaba Cloud.

How can I use Security Center to protect my servers in on-premises data centers and third-party cloud servers?

Before you use Security Center to protect the servers in on-premises data centers and third-party cloud servers, you must install the Security Center agent on these servers. For more information, see the following table.

Server type	How to use Security Center to protect the servers
Alibaba Cloud ECS	If you select **Security Enhancement** when you purchase an ECS instance, the Security Center agent is automatically installed and the Basic edition of Security Center is automatically activated. The Basic edition is provided free of charge. **Note** The Basic edition of Security Center only detects unusual logons and urgent vulnerabilities. The Basic edition is suitable for individual developers.

Server type	How to use Security Center to protect the servers
instances	If you do not select **Security Enhancement** when you purchase an ECS instance, or Security Center prompts that **the Security Center agent is offline**, perform the following operations to enable Security Center to protect the ECS instance: 1. Upgrade Security Center to the Basic Anti-Virus, Advanced, or Enterprise edition. For more information, see Purchase Security Center. **Note** The Basic edition of Security Center only detects unusual logons and urgent vulnerabilities. The Basic edition is suitable for individual developers. 2. Log on to the Security Center console. 3. Install the Security Center agent on the ECS instance in the Security Center console. For more information, see Manually install the Security Center agent.
Cloud servers from third-parties Servers in on-premises data centers	To enable Security Center to protect the third-party cloud servers, perform the following operations: 1. Upgrade Security Center to the Basic Anti-Virus, Advanced, or Enterprise edition. For more information, see Purchase Security Center. **Note** The Basic edition of Security Center only detects unusual logons and urgent vulnerabilities. The Basic edition is suitable for individual developers. 2. Log on to the Security Center console. 3. Install the Security Center agent on the ECS instance in the Security Center console. For more information, see Manually install the Security Center agent. 4.

If I have 100 ECS instances, can I activate Security Center for only 10 ECS instances?

No, if you have purchased the Basic Anti-Virus, Advanced, or Enterprise edition of Security Center, you must activate Security Center for all the ECS instances under your current account.

When you purchase the Basic Anti-Virus, Advanced, or Enterprise edition of Security Center, you must specify **Protected Servers**. The number of Protected Servers represents the total number of servers under your Alibaba Cloud account. The default value is the total number of your Alibaba Cloud ECS instances and third-party cloud servers that have the Security Center agent installed.

Does Security Center provide the antivirus service?

Yes, the Basic Anti-Virus, Advanced, or Enterprise edition of Security Center detects and automatically removes common viruses. For more information, see The anti-virus feature.

Which edition of Security Center provides the automatic vulnerability fix feature?

The Advanced and Enterprise editions support automatic vulnerability fix.

Which edition of Security Center do I select if I want to meet the testing and evaluation requirements for classified protection?

You must purchase the **Enterprise** edition of Security Center and enable log analysis, which is a value-added service. For more information about how to enable log analysis, see Activate log analysis.

> **Note** The Enterprise edition of Security Center supports baseline checks. You can use this feature in combination with log analysis, which retains log data for 180 days, to meet the testing and evaluation requirements for classified protection.

8.Terms

This topic provides commonly used terms of Security Center.

privilege escalation

Attackers may exploit the privilege escalation vulnerability to obtain the highest permissions and control the website server during attacks. Attackers may exploit this vulnerability to break through the security defense system and threaten assets and data security.

code execution

Attackers may run malicious code on servers to attack or control them.

CVSS

The common vulnerability scoring system (CVSS) is used to assess the severity of vulnerabilities.

DDoS

A distributed denial of service (DDoS) attack is a malicious attempt to attack one or more targets by using multiple compromised computer systems. This type of attack poses great threats to servers.

Web CMS

Security Center provides the web content management system (Web CMS) feature that uses content repositories or databases to store page content, metadata, or other information assets that a system requires.

vulnerability

Vulnerabilities refer to flaws in operating system implementation or security policies. Attackers can exploit vulnerabilities to access the data on your servers or undermine the security of your servers. We recommend that you fix detected vulnerabilities in a timely manner to protect your assets.

baseline

A baseline describes the minimum security requirements for system configuration and management.The following items are considered baselines: service and application configurations, configurations for operating system components, permission settings, and system management rules.