Alibaba Cloud Threat Detection

Product Introduction

Issue: 20190920

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 due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
⛔	This warning information 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.
⚠	This warning information 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 restore business.
📋	This indicates warning information, supplementary instructions, and other content that the user must understand.	❗ Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	📋 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
`Italics`	It is used for parameters and variables.	`bae log list --instanceid` *`Instance_ID`*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *`[-all|-t]`*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *{stand | slave}*

Contents

1 What is Security Center?

Alibaba Security offers Security Center (original name: Threat Detection Service) to secure and monitor diagnostics services. Security Center supports multiple features, including security event detection, vulnerability scanning, and configuration baseline check. You can use Security Center to secure and manage your assets on the cloud . With the integration of Alibaba's independently developed big data and machine learning algorithm, Security Center can help you check and process all the security threats in real time.

Security Center also enables you to analyze the security situation and detect potential threats by collecting and auditing up to 10 types of security logs, your asset fingerprints, and network threat intelligence.

Features of Security Center

Security Center supports the following features:

- Security events and automatic alert correlation analysis: Security Center detects common network intrusions in real time, such as unusual logons, Webshell injections, unusual server activities and virus attacks. It generates alert for detected events, and automatically correlates unusual alarm events to help you fully understand and analyze corresponding threats and intrusion events.
- Vulnerability scanning: Security Center automatically scans for vulnerabilities on servers and provides fixes. It can also eliminate vulnerabilities for web content management systems (WCMS) , Linux, and Windows.
- Baseline check: Security Center periodically checks the server configuration using either the default or customized scan policies. The baseline check includes security compliance check, system configuration check, account check, and weak password check.
- Asset fingerprints: Collects and records asset running information, including processes, system accounts, open ports, software versions, and website background information.
- Log retrieval: Security Center provides an all-in-one log retrieval service for you to query and manage up to 10 types of server and web logs so that you can track the causes of security issues.

2 Benefits of Security Center

Alibaba Security Center can help to build a complete cloud security system that supports security events monitoring, vulnerability detection, baseline check, asset fingerprints, and log retrieval. Security Center monitors web intrusions in real time and generates security alerts when an intrusion is detected. Vulnerability detection and baseline check are used to check and fix system flaws to prevent potential attacks. Asset fingerprints update you information on server processes, your system accounts, software and listening ports. Log retrieval provides server logs and network logs to help you analyze the security trends of your servers, track the causes of security events and help you handle the security threats detected by Security Center.

Security Center has the following benefits:

- Security alerts and alert correlation

  Security Center detects security issues in real time, provides solutions, and allows you to search and analyze logs and events. Alert correlation rules automatically group the related events together and then generate a related alert. It can help you see all the related alerts on one page, and provide you with centralized management on the alerts and related events.
- Vulnerability detection and baseline check

  Security Center automatically detects vulnerabilities and insecure configurations on assets, and provides solutions to enhance system security.
- Risk quantification and prediction

  Security Center uses machine learning to quantify and analyze the threats, and predict potential risks.
- Visualized user interface

  Security Center provides a visualized user interface for you to view security issues at any time.
- Log storage and retrieval

  Security Center provides you with the last 180 days' log and allows you to search and analyze logs created in the last 30 days.

- Overall log analysis

  Security Center provides real-time log search and analysis, which covers all types of logs for Security Center, such as starting of server process, outgoing network connection, system logon, DNS request, etc. Supports the creation of reports and alarms.

Cloud Threat Detection

Cloud Threat Detection integrates the features of popular antivirus engines, and provides you with comprehensive and real-time virus detection and protection service. This service features a unique detection model, which is based on machine learning and deep learning techniques, and large amount of threat information gathered by Alibaba Cloud.

Cloud Threat Detection checks hundreds of millions of files every day and serves millions of cloud servers.

Detection capabilities of Cloud Threat Detection

Security Center collects the process information on servers and upload it onto cloud for viruses detection. If a malicious process has been detected, you can directly stop the process and quarantine the related files.

- Virus detection engine (self-developed by Alibaba) is built on deep learning techniques and a large amount of attack samples and protection policies. The engine specializes in detecting malicious files in the cloud, can effectively identify potential threats, and cover the shortages of traditional antivirus engines.
- Cloud sandbox (self-developed by Alibaba) simulates cloud environments and allow you to monitor attacks from malicious samples. Based on big data analysis and machine learning modeling techniques, cloud sandbox automatically checks and detects potential threats and offers dynamic analysis and detection capabilities.
- Integration with antivirus engines popular in the world enables the service to timely update the virus database.
- Based on the threat data provided by Security Center, the service also integrates a server detection model to detect suspicious processes and malicious activities from various perspectives.

Supported virus types

Cloud Threat Detection provides a comprehensive solution based on the experience of Alibaba Cloud's security and defense experts. It covers data collection, masking, recognition, analysis, quarantine and recovery. You can quarantine malicious files and restore quarantined files on Security Center console.

Cloud Threat Detection can detect the following virus types :

Virus	Description
Mining program	A mining program illegally consumes server resources to mine virtual currencies.
Computer worm	A computer worm is a malware computer program that replicates itself and spread to a large number of computers within a short time.
Ransomware	Ransomware such as WannaCry uses encryption algorithms to encrypt files and prevent users from accessing their files.
Trojans	A trojan is a malicious program that allows the attacker to access users' personal information, to gain control of the server, and to consume system resources.
DDoS trojan	A DDoS trojan hijacks servers and uses zombie servers to launch DDoS attacks, which can interrupt your normal service.
Backdoor	A backdoor is a malicious program injected by an attacker, who uses the backdoor to control the server or launch attacks.
Computer virus	A computer virus is a type of malicious program that can replicate itself by modifying other programs and insert malicious code into other programs to infect the whole system.
Malicious program	Programs that brings harm to a computer system and data security.

3 Features

Security Center is available in Basic, Advanced and Enterprise Edition.

- Basic Edition: Detects unusual logon and server vulnerabilities. Basic Edition is available for free.
- Enterprise Edition: Provides comprehensive security services, including security events, server vulnerability detection and resolution, baseline check, asset fingerprints, and log retrieval. Enterprise Edition is charged by annual and monthly subscription.

Feature comparison among Basic/Advanced/Enterprise Edition

The following table compares the features provided by Basic Edition, Advanced Edition and Enterprise Edition of Security Center:

- X indicates that the related feature is excluded in the service.
- √ indicates that the related feature is included in the service.
- Value-added indicates that you must purchase the related feature additionally.

Note:
Basic Edition detects unusual logon and server vulnerabilities. Basic Edition is available for free. Advanced and Enterprise Edition provides comprehensive security services, and they are charged by annual and monthly subscription.

Feature	Item	Description	Basic	Advance	Enterprise
Security events	Unusual logon detection	Basic detection · Logon from unusual locations: Security Center automatically records locations that are commonly used to log on to Elastic Compute Service (ECS) instances. You can also manually specify these locations in Security Center console. The system will generate an alarm when a logon from an unusual location is detected. · Brute-force cracking: Security Center detects a logon to ECS instances after multiple failed attempts, which may be caused by brute-force password cracking.	√	√	√
		Advanced detection · Invalid IP logon: This feature allows you to configure valid IP addresses for logging on to ECS instances, such as bastion host IP addresses and local area network (LAN) IP addresses. Therefore, this system generates an alarm when detecting a logon with an unspecified IP address . · Invalid account logon: This feature allows you to specify the valid accounts for logging on to ECS instances. Therefore, this system generates an alarm when detecting a logon with an unspecified account. · Logon during invalid periods: This feature allows you to specify valid periods, such as office hours , for logging on to ECS instances. Therefore, this system generates an alarm when detecting a logon that does not occur during the specified period.	X	√	√

Feature	Item	Description	Basic	Advance	Enterprise
Security events	Webshell removal	Webshell detection: checks both instances/servers and networks for web scripts, such as PHP, ASP, and JSP files. · Instance check: monitors the changes of Web directories on an instance in real time. · Network check: simulates Webshell execution and analyzes network protocols.	X	√	√
		Webshell removal: easily quarantines the detected Webshell in the console. You can restore the Webshell within 30 days after isolation.	X	√	√

Feature	Item	Description	Basic	Advance	Enterprise
	Malicious processes (malware checking)	Virus detection: Periodically scans processes, monitors process initiation events, and detects malicious viruses and Trojans using the anti-virus mechanism in the cloud. Virus removal: Terminates processes and quarantines malicious files in the console. Scope of virus targets: · Ransomware: File-encrypting ransomware such as WannaCry and CryptoLocker. · Malicious attacks: Distributed Denial-of-Service (DDoS) Trojans , malicious scanning Trojans, and spam Trojans. · Mining software: Resource consumption software that uses instances for illegal virtual currency mining. · Zombies: Central control Trojans, malicious central control connection s, and hacking tools. · Other viruses: Worms, Mirai, and infectious viruses. Virus database: · Update mechanism: Updates the virus management in the cloud, and does not provide any on-premises detection engine. · Virus sample coverage: Detects all types of viruses, and integrates the worldwide major anti-virus engines , proprietary sandbox, and machine learning engine in the cloud.	X	√	√

Feature	Item	Description	Basic	Advance	Enterprise
	Suspicious processes	Suspicious process detection: Restores intrusion links based on real attack-defense scenarios in the cloud, creates a process whitelist, and generates alarms when detecting illegal and intrusive processes. Scope of suspicious types: · Reverse shell: Suspicious commands in Bash processes, and arbitrary commands remotely executed by instances. · Suspicious database commands: Suspicious commands in databases , such as MySQL, PostgreSQL, SQLServer, Redis, and Oracle. · Illegal operations in application processes: Illegal operations in process such as Java, FTP, Tomcat, Docker containers, and Lsass.exe. · Illegal system processes: PowerShell , Secure Shell (SSH), Remote Desktop Protocol (RDP), smbd, and secure copy protocol (SCP). · Other suspicious processes: Visual Basic Script (VBScript) execution, accessing instances, writing crontab files, and Webshell injection. Suspicious process coverage: Builds more than 1,000 process patterns for hundreds of processes, and analyzes suspicious processes by comparing them with these patterns.	X	√	√

Feature	Item	Description	Basic	Advanc	Enterprise
	Sensitive file tampering	Tampering detection: Monitors sensitive directories and files in real time, and generates alarms when detecting suspicious reading, writing, and deletion processes.Scope of tampering detection: · System file tampering: Malicious replacement of processes that run Bash and ps commands, and operation of hidden illegal processes . · Core dump removal: Malicious removal of website core dump files after an illegal logon to instances. · Drive-by downloading: Malicious code injection into a Web page that causes the auto downloading of Trojans. · Other suspicious events: Ransomware on the logon pages of Linux and MysqlDB, creating emails or Bitcoin wallet addresses.	X	√	√
	Unusual network connectio	Unusual connection: Monitors connections between instances and networks, and generates an alarm when detecting an illegal connection.Scope of unusual connections: · Active connections to unknown servers: Active connections to suspicious IP addresses using reverse shell and Bash commands. · Malicious attacks: Malicious software injection used to launch malicious attacks, such as SYN floods , User Datagram Protocol (UDP) floods, and Internet Control Message Protocol (ICMP) floods. · Suspicious communications: Suspicious Webshell communicat ions.	X	√	√

Feature	Item	Description	Basic	Advance	Enterprise
Vulnerability management	Vulnerabilities of Linux software	Detection of Linux software vulnerabilities: Compares software versions by using the Open Vulnerability and Assessment Language (OVAL®) matching engine, and generates alarms when detecting vulnerabilities from the Common Vulnerabilities and Exposures (CVE®) vulnerability database.	√	√	√
		Vulnerability fix: Fixes vulnerabilities automatically with easily applied updates, and generates vulnerability fix instructions for manual fixes.	X	√	√
	Windows vulnerabilities	Detection of Windows vulnerabilities: Obtains updates from Microsoft Updates for the Windows operating system, detects critical and other vulnerabilities, and generates alarms of these vulnerabilities.	√	√	√
		Vulnerability fix: Downloads updates, installs the updates silently, and then prompts you to restart the system if required.	X	√	√
	WCMS vulnerabilities	Detection of Web content management system (WCMS) vulnerabilities: Monitors Web directories, recognizes common website builders, and checks the vulnerability database to identify vulnerabilities in the website builders.	√	√	√
		Vulnerability fix: Uses proprietary updates developed by Alibaba Cloud to replace or modify source code and allows you to easily fix vulnerabilities.	X	√	√

Feature	Item	Description	Basic	Advance	Enterprise
Baseline check	Server baseline	Server baseline check: Initiates tasks to scan security configurations of servers, and generates notifications for vulnerable configurations. Scope of server baseline check: · Account security: Password policy compliance, and weak passwords of systems and applications. · System configurations: Potential risks in group policies, logon baseline policies, and registry configurations. · Databases: Critical threats in the configurations of databases such as Redis. · Compliance requirements: Compliance with system baseline requirements, such as the CIS-Linux Centos7 benchmark. Check policy: Supports a customized check policy that specifies the checked items, check cycle, and target server group. The system does not support customized check scripts.	X	X	√

Feature	Item	Description	Basic	Advance	Enterprise
Asset fingerprints	Asset fingerprints	Port: Collects and displays port listening information, and records changes to track opened ports. Account: Collects information about accounts and related permissions, and checks privileged accounts for privilege elevation. Process: Collects and displays process snapshots to track normal processes and detect unusual processes. Software: Checks software installation information, and in the case of critical vulnerabilities, quickly locates affected assets. Website background: Recognizes website back-end assets, and detects user enumeration attempts and unusual background logons.	X	X	√
Log analysis	Overall log analysis	Security Center provides real-time log search and analysis, which covers all types of logs for Security Center, such as starting of server process, outgoing network connection, system logon, DNS request, etc.	X	Value-added	Value-added
Web Guard	Web Guard	Web Guards adopts the advanced web tempering protection technology, monitors the protected directories , prevents your website providing illegally tempered information, and backup and restore the website files.	X	Value-added	Value-added

Feature	Item	Description	Basic	Advance	Enterprise
Alert correlation analysis	Alert correlation analysis	Alert correlation rules automatically group the related events together and then generate a related alert. It can help you see all the related alerts on one page, and provide you with centralized management on the alerts and related events.	X	X	√

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 configurat ions, 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

All logs of Security Center are stored in dedicated Logstores.

Logstore limits

- You cannot use the Log Service API or SDK to write data into the Logstores or modify the attributes of a Logstore, such as the storage period.
- Dedicated Logstores have no limits on queries, statistics, alerts, and stream consumption.
- Dedicated Logstores do not incur charges on the condition that Log Service functions normally.
- The default reports may be updated later.