

Alibaba Cloud 云安全中心（安骑士）

User Guide

Issue: 20200605









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 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 contact Alibaba Cloud directly if you discover any errors in this document.

Document conventions

Style	Description	Example
	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.
	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.
	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.
	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 <code>cd /d C:/window</code> command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
{ } or {a b}	This format is used for a required value, where only one item can be selected.	switch {active stand}

Contents

Legal disclaimer.....	I
Document conventions.....	I
1 intrusion detection.....	1
1.1 Server exceptions.....	1
1.1.1 Virus removal.....	1

1 intrusion detection

1.1 Server exceptions

1.1.1 Virus removal

The virus removal feature provided by Server Guard is integrated with major antivirus engines worldwide. It detects viruses against large amounts of threat intelligence data provided by Alibaba Cloud. Virus removal also provides an exception detection module designed by Alibaba Cloud to detect viruses based on machine learning and deep learning. With these features, virus removal can provide full-scale and dynamic antivirus protection to safeguard your servers.

The cloud threat detection feature can scan millions of files on a daily basis and is currently protecting millions of assets on the cloud.

Detection capabilities

The virus removal feature uses the Server Guard client to collect process information, and then scans the retrieved data for viruses in the cloud. If a malicious process is detected, you can directly stop the process and quarantine the related files.

- **Deep learning engine (developed by Alibaba Cloud):** The deep learning engine is built on deep learning technology and a large amount of attack samples. The engine specializes in detecting malicious files in the cloud and automatically identifies potential threats. It provides additional detection capabilities compared to traditional antivirus engines.
- **Cloud sandbox (developed by Alibaba Cloud):** It allows you to simulate cloud environments and monitor attacks launched by malicious samples. Based on big data analytics and machine learning modeling techniques, cloud sandbox automatically detects threats and offers dynamic analysis and detection capabilities.
- **Integration with major antivirus engines:** The cloud threat detection feature is integrated with major antivirus engines worldwide. Its virus library is updated in real time.
- **Threat intelligence detection:** Based on the threat intelligence data provided by Alibaba Cloud Security, cloud threat detection works with the exception detection module to detect malicious processes and operations.

Detectable virus types

Cloud threat detection is one of the best practices tested by Alibaba Cloud Security technologies and specialists. It provides end-to-end security services, including threat intelligence collection, data masking, threat identification, threat analysis, and malicious file quarantine and restoration. You can quarantine and restore data that has viruses in the Security Center console.

Cloud threat detection can detect the following types of viruses:

Virus	Description
Mining programs	A mining program consumes server resources without authorization to mine virtual currencies.
Computer worms	A computer worm uses computer networks to replicate itself and spread to a large number of computers within a short period of time.
Ransomware	Ransomware, such as WannaCry, uses encryption algorithms to encrypt files and prevent users from accessing the files.
Trojans	A Trojan is a program that allows the attacker to access information about the server and users, to gain control of the server, and to consume system resources.
DDoS Trojans	A DDoS Trojan hijacks servers and uses zombie servers to launch DDoS attacks, which can interrupt your workloads.
Backdoors	A backdoor is a malicious program injected by an attacker, who uses the backdoor to control the server or launch attacks.
Computer viruses	A computer virus inserts malicious code into other programs, and may replicate and infect the whole system.
Malicious programs	Programs that may pose a threat to the system and data security.

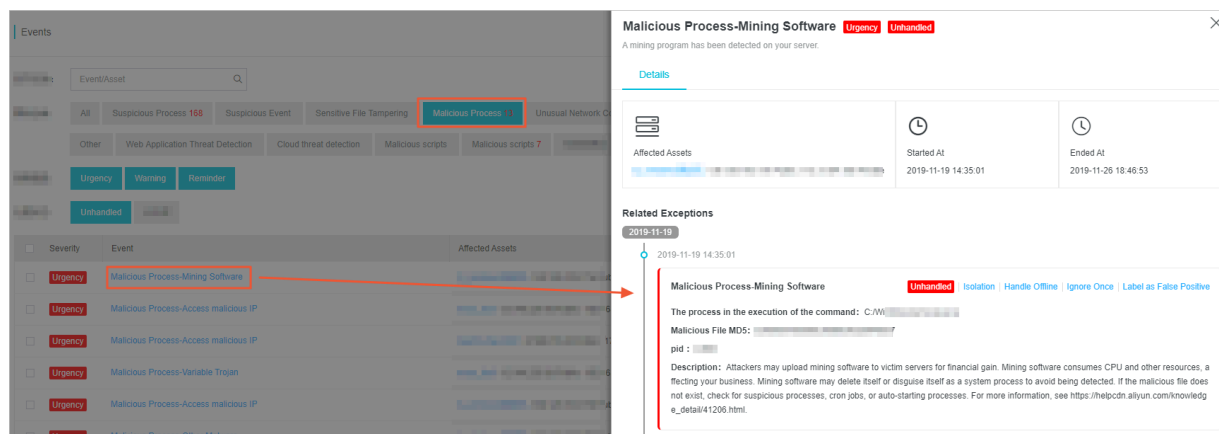
Benefits

- **Independent development and controllability:** Cloud threat detection is based on deep learning, machine learning, and big data analytics with a large amount of attack and defense practices. It uses multiple detection engines to protect your assets against viruses without delay.
- **Lightweight:** Cloud threat detection only takes 1% CPU usage and 50 MB of memory.
- **Dynamic:** Cloud threat detection dynamically retrieves log data to monitor the launches of malicious programs.

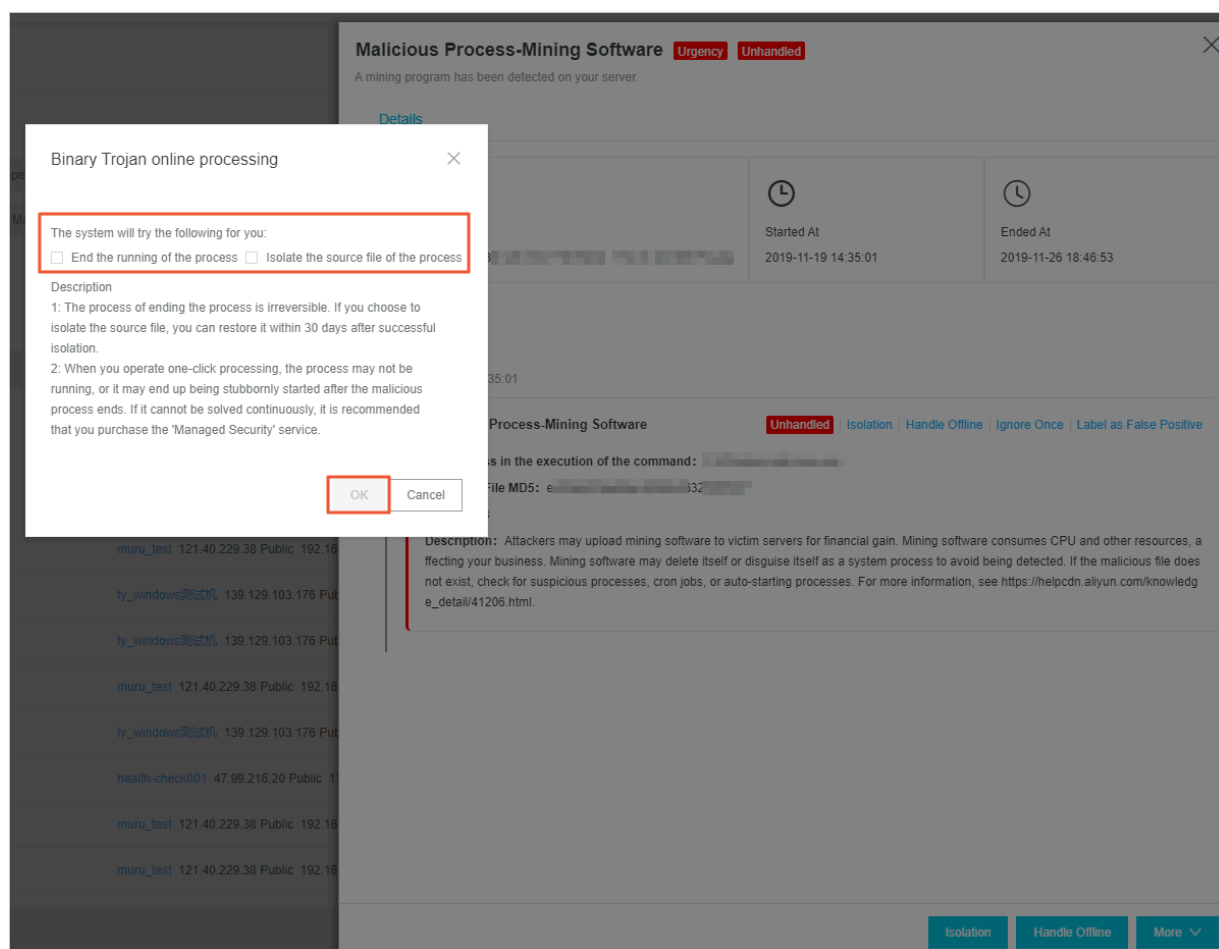
- **Easy to manage:** You can manage all servers and view their status at any time in the Security Center console.

Scenarios



Detection



Quarantine



Restoration

Quarantine				
 The system only keeps a quarantined file for 30 days. You can restore any quarantined file before the system deletes the file.				
Host	Path	Status 	Modified At	Actions
192.168.1.101	C:\Program Files\Internet Explorer\iexplore.exe	Quarantined	2019-11-14 18:04:43	Restore
192.168.1.101	C:\Program Files\Internet Explorer\iexplore.exe	Quarantined	2019-11-14 17:59:25	Restore
192.168.1.101	C:\Program Files\Internet Explorer\iexplore.exe	Restoration Failed	2019-11-14 17:44:46	Restore
192.168.1.101	C:\Program Files\Internet Explorer\iexplore.exe	Quarantined	2019-11-14 16:58:31	Restore
192.168.1.101	C:\Program Files\Internet Explorer\iexplore.exe	Restored	2019-11-14 16:53:26	--
192.168.1.101	C:\Program Files\Internet Explorer\iexplore.exe	Quarantined	2019-11-06 09:30:11	Restore
192.168.1.101	C:\Program Files\Internet Explorer\iexplore.exe	Quarantined	2019-11-05 19:18:09	Restore
192.168.1.101	C:\Program Files\Internet Explorer\iexplore.exe	Quarantined	2019-10-29 14:02:54	Restore
				< Previous 1 Next >