Privacy and Sample Visibility for Secure Malware Analytics

First Published: 2023-08-29

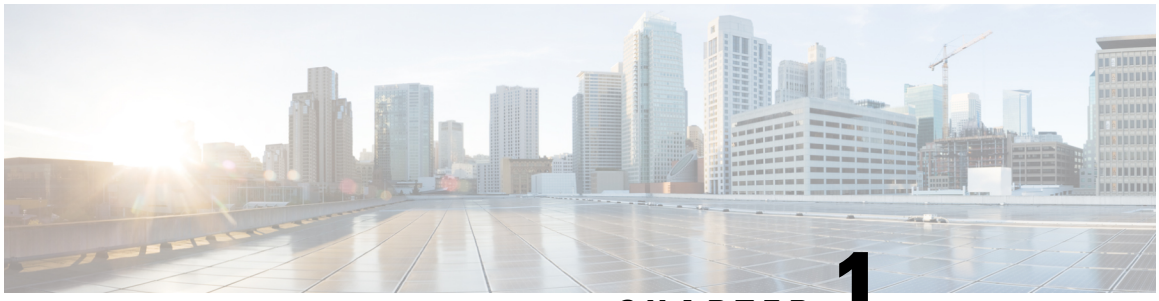
Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1 **Privacy and Sample Visibility** 1

Privacy and Visibility on Secure Malware Analytics Appliances 1

Privacy and Visibility on the Secure Malware Analytics Cloud 2



CHAPTER 1

Privacy and Sample Visibility

When submitting samples to Secure Malware Analytics for analysis, an important consideration is the privacy of their contents. Privacy is a particularly important consideration if sensitive documents or archive types are submitted for analysis, because locating sensitive material could be relatively easy for those with access to Secure Malware Analytics, especially with the search API.

Privacy may be less of a concern when submitting samples to an on-premises Secure Malware Analytics Appliance than to the Secure Malware Analytics Cloud, but understanding the basics of privacy and sample visibility is still necessary for Secure Malware Analytics Appliance administrators.

The privacy and sample visibility model for sample submissions to Secure Malware Analytics is relatively simple: Unless samples are designated as Private, they will be visible to users who are outside the submitter's Organization. In general, a sample designated as *Private* may only be seen by Secure Malware Analytics users within the same Organization as the user who submitted the sample.

- Privacy and Visibility on Secure Malware Analytics Appliances , on page 1
- Privacy and Visibility on the Secure Malware Analytics Cloud , on page 2

Privacy and Visibility on Secure Malware Analytics Appliances

The privacy and sample visibility model is modified on Secure Malware Analytics Appliances for samples that are submitted by "CSA Integrations". CSA Integrations are Cisco products such as ESA/WSA appliances and other devices or services, which are integrated (registered) with Secure Malware Analytics Appliances via the CSA API.

All sample submissions on Secure Malware Analytics Appliances are Public by default, and can be viewed by any other appliance user, including CSA Integrations, regardless of which Organization they belong to.

All appliance users can see all details of samples submitted by all other users.

Non-CSA Secure Malware Analytics users may submit Private samples to the Secure Malware Analytics Appliance, in which case the samples are only visible to other Secure Malware Analytics Appliance users, including CSA Integrations, within the submitter's Organization.

Privacy and sample visibility model on Secure Malware Analytics Appliances illustrated in the table below, using the following terms:

CSA Integrations	CSA Integrations are ESA/WSA appliances and other Cisco devices or services that are registered on a Secure Malware Analytics Appliance via the CSA API. Samples submitted to Secure Malware Analytics Appliances by CSA Integrations are Public by default.

Other Integrations	The same basic privacy rules apply to other integrations such as FireAMP Private Cloud.
Secure Malware Analytics User - Public	Public samples submitted to a Secure Malware Analytics Appliance bynormal Secure Malware Analytics users (i.e., non-CSA Integrations). For example, appliance administrators or malware analysts who submit samples via the Secure Malware Analytics Portal UI, or by using the Secure Malware Analytics Native API.
Secure Malware Analytics User - Private	Private samples submitted to a Secure Malware Analytics Appliance by normal Secure Malware Analytics users. In this case, the Private samples are invisible to all other users on the appliance who are outside of the submitter's Organization. (The samples will be visible to CSA Integrations within the same Organization as the submitter.)

Table 1: Privacy and Visibility on Secure Malware Analytics Appliances

	Sample Visibility when Accessed by:			
Sample Submitted by:	**Secure Malware Analytics Users from the Same Organization**	**Secure Malware Analytics Users from a Different Organization**	**CSA Integration from the Same Organization**	**CSA Integration from a Different Organization**
Secure Malware Analytics User - Public	Full	Full	Full	Full
Secure Malware Analytics User - Private	Full	None	Full	None
CSA Integration (ESA/WSA appliances, etc.) **All CSA submissions to Secure Malware Analytics Appliance are public by default**	Full	Full	Full	Full

The same basic privacy rules apply to Secure Malware Analytics Appliance integrations with FireAMP Private Cloud.

Privacy and Visibility on the Secure Malware Analytics Cloud

If a Private sample is submitted to the Secure Malware Analytics Cloud via the Cisco Sandbox API ("CSA API"), then a "scrubbed" version (with limited elements) can be shared with other CSA Integrations.

The following table illustrates sample privacy and visibility on the Secure Malware Analytics Cloud:

Note In scrubbed reports, all potentially sensitive information about the sample is removed. There are no filenames, no process names, etc. Samples may not be downloaded.

Table 2: Privacy and Visibility on the Secure Malware Analytics Cloud

	Sample Visibility when Accessed by:			
Sample Submitted by:	**Secure Malware Analytics Users from the Same Organization**	**Secure Malware Analytics Users from a Different Organization**	**CSA Integration from the Same Organization**	**CSA Integration from a Different Organization**
Secure Malware Analytics User - Public	Full	Full	Full	Scrubbed
Secure Malware Analytics User - Private	Full	None	Full	None
CSA Integration (ESA/WSA appliances, etc.) **All CSA submissions to Secure Malware Analytics Cloud are private by default**	Full	None	Full	Scrubbed

For more information, see the documentation on the Secure Malware Analytics Install and Upgrades page on cisco.com.