ThreatQuotient

A Securonix Company



IPQS Malware And Virus File Scanner Operation

Version 1.0.0

November 20, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@securonix.com
Web: https://ts.securonix.com
Phone: 703.574.9893

Contents

Warning and Disclaimer **3**
Support **4**
Integration Details **5**
Introduction **6**
Prerequisites **7**
Installation **8**
Configuration **9**
Actions **10**
Malware File Scan 11
Malware Scan Result 13
Run Configuration Options 14
Change Log **15**

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2026 ThreatQuotient, Inc.
All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@securonix.com
Support Web: https://ts.securonix.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ⚠ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.29.0
Support Tier	ThreatQ Supported

Introduction

The IPQS Malware And Virus File Scanner Operation scans URLs and ThreatQ attachments for malware and viruses using IPQualityScore (IPQS) detection engines. It checks for a stored result from the last 24 hours before starting a fresh scan and returns scan data as attributes and detection engine results.

The operation provides the following actions:

- **Malware File Scan** - Looks up a recent result, then starts a fresh scan when the successful lookup has no detection engine results.
- **Malware Scan Result** - Retrieves a pending scan result using its Request ID.

The operation is compatible with the following system objects:

- Indicator
- URL
- Attachments

Prerequisites

The following is required to run the operation:

- An IPQS API Key

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the integration file on your local machine

    > ThreatQ will inform you if the operation already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the operation contains changes to the user configuration. The new user configurations will overwrite the existing ones for the operation and will require user confirmation before proceeding.

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

Configuration

ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
IPQualityScore API Key	Your IPQualityScore API key with access to the Malware File Scanner API.

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Malware File Scan	Looks up a stored result, then starts a fresh scan when needed.	Indicator, Attachment	URL, All attachment types
Malware Scan Result	Retrieves a scan result using its Request ID.	Indicator, Attachment	URL, All attachment types

Malware File Scan

The Malware File Scan action scans the file at a URL or the content of an attachment. It first requests a stored IPQS result from the previous 24 hours. If the lookup succeeds but has no detection engine results, it starts a fresh scan. If the lookup fails, the IPQS error message is returned and a new scan is not started.

For a URL, IPQS fetches the file at the URL. For an attachment, the operation downloads the attachment from ThreatQ and uploads it to IPQS. A malware-locked ZIP containing one file is unpacked with the password `infected` before upload.

`POST https://www.ipqualityscore.com/api/json/malware/lookup` - Checks for a stored result from the last 24 hours.

`POST https://www.ipqualityscore.com/api/json/malware/scan` - Starts a fresh scan when the lookup succeeds but returns no detection results.

URLs are sent as a form field; attachments are sent as multipart file uploads. IPQS keeps scan results for 24 hours. Because the content behind a URL can change, IPQS may scan it again.

Sample Response (Cached Lookup, Truncated):


```
{
  "success": true,
  "message": "Success",
  "file_name": "www.example.com",
  "file_hash":
"bf7217917644a8b08727b48deb0df9f9b06ca3b6817bd597edc5821ec3134607",
  "type": "lookup",
  "status": "cached",
  "detected": false,
  "total_scans": 0,
  "detected_scans": 0,
  "result": [
    {
      "name": "IPQS Internet Security Suite",
      "detected": false,
      "error": false
    }
  ],
  "file_size": 577,
  "file_type": "text/html",
  "request_id": "<request_id>"
```

```
}
```

If a fresh scan is pending, its Request ID is saved as the object's `IPQS: Request ID` attribute. Run `malware_scan_result` later to retrieve the result. If saving the attribute fails, the Request ID is available in the operation output and can be entered manually in `malware_scan_result`.

ThreatQ provides the following default mapping for this Action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
status	Attribute	IPQS: Scan Status	N/A	cached	Status returned by the lookup; a pending fresh scan may return pending.
request_id	Attribute	IPQS: Request ID	N/A	Request ID string	Included in the result; saved automatically when a fresh scan is pending.
type	Attribute	IPQS: Scan Type	N/A	lookup	Identifies this response as a stored lookup.
file_name	Attribute	IPQS: File Name	N/A	www.example.com	Filename or URL returned by IPQS.
file_type	Attribute	IPQS: File Type	N/A	text/html	MIME type returned by IPQS.
file_size	Attribute	IPQS: File Size	N/A	577	File size in bytes.
file_hash	Attribute	IPQS: File Hash	N/A	SHA-256 hash	SHA-256 hash returned by IPQS.
md5, sha1	Attributes	IPQS: MD5, IPQS: SHA-1	N/A	Hash strings	Hashes returned by the lookup.
detected	Attribute	IPQS: Detected	N/A	false	Whether any engine detected the file.
detected_scans, total_scans	Attributes	IPQS: Detected Scans, IPQS: Total Scans	N/A	0	Counts returned by the lookup.
message	Attribute	IPQS: Message	N/A	IPQS error text	Displayed instead of normal response attributes when the request fails.

Malware Scan Result

This action retrieves an earlier scan result by Request ID. It uses the Request ID entered for the action or the most recently saved `IPQS: Request ID` attribute on the object. If no ID is available, the operation asks the user to run a scan first or enter an ID.

`GET https://www.ipqualityscore.com/api/json/postback?request_id=<request_id>`

While the result is pending, the operation makes up to three requests, five seconds apart. If it remains pending, run the action again later.

Sample Response:

```
{
  "success": true,
  "file_name": "www.example.com",
  "type": "scan",
  "status": "done",
  "detected": false,
  "detected_scans": 0,
  "total_scans": 7,
  "result": [
    {
      "name": "IPQS Internet Security Suite",
      "detected": false,
      "error": false
    }
  ],
  "scan_date": {
    "date": "2026-11-17 08:16:46.000000",
    "timezone": "America/New_York"
  },
  "flagged": false,
  "tainted": false,
  "request_id": "<request_id>"
}
```

ThreatQ provides the following default mapping for this Action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`status`	`Attribute`	`IPQS: Scan Status`	`N/A`	`done, pending`	`Scan status returned by IPQS.`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
request_id	Attribute	IPQS: Request ID	N/A	Request ID string	Identifier used to retrieve the scan result.
type	Attribute	IPQS: Scan Type	N/A	scan	Type of scan associated with the result.
file_name	Attribute	IPQS: File Name	N/A	www.example.com	Filename or URL returned by IPQS.
file_type	Attribute	IPQS: File Type	N/A	text/html	MIME type returned by IPQS.
file_size	Attribute	IPQS: File Size	N/A	577	File size in bytes.
file_hash	Attribute	IPQS: File Hash	N/A	SHA-256 hash	SHA-256 hash returned by IPQS.
md5	Attribute	IPQS: MD5	N/A	MD5 hash	MD5 hash returned by IPQS.
sha1	Attribute	IPQS: SHA-1	N/A	SHA-1 hash	SHA-1 hash returned by IPQS.
detected	Attribute	IPQS: Detected	N/A	false	Whether any engine detected the file.
detected_scans	Attribute	IPQS: Detected Scans	N/A	0	Number of engines that detected the file.
total_scans	Attribute	IPQS: Total Scans	N/A	7	Number of engines that scanned the file.
flagged	Attribute	IPQS: Flagged	N/A	false	Whether IPQS flagged the file.
tainted	Attribute	IPQS: Tainted	N/A	false	Whether IPQS marked the file as tainted.
scan_date.date, scan_date.timezone	Attributes	IPQS: Scan Date, IPQS: Scan Date Timezone	N/A	Date string, America/New_York	Flattened from the IPQS scan_date object.
message	Attribute	IPQS: Message	N/A	IPQS error text	Displayed instead of normal response attributes when the request fails.

Run Configuration Options

These configuration options are set after selecting the action to run against an object and are not set from the operation's configuration screen.

The following run option is available when you select the Malware Scan Result action:

PARAMETER	DESCRIPTION
Request ID (optional)	Leave blank to use the saved `IPQS: Request ID` attribute. Enter a Request ID to override it.

Change Log

- **Version 1.0.0**
  - Initial release