Qualys Container Security

API Release Notes

Version 1.28

August 14, 2023

Qualys Cloud Suite API gives you many ways to integrate your programs and API calls with Qualys capabilities. You'll find all the details in our user guides, available at the time of release. Just log in to your Qualys account and go to Help > Resources.

What's New

Malware Detection

Image Details with Malware and Secrets Information

Expiration Date for Reports

Qualys API URL

The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

Click here to identify your Qualys platform and get the API URL

Malware Detection

With this release, we are introducing malware detection in Container Security. This adds an extra layer of security and ensures your infrastructure and data remain secure. The following new APIs have been introduced to view malware information for container images:

Show Detected Malwares for Image

Show Detected Malware Files for an Image Layer

The following API has been updated to show malware information in image details:

Show Details of an Image

Fetch a List of Images (Bulk API)

Show Malwares Detected for an Image

API affected	/images/{imageSha}/layers/malware
Operator	GET
New or Updated APIs	New

Shows a list of malwares detected for all layers of an image.

Input Parameters

Parameter	Mandatory?	Data Type	Description
imageSha	Mandatory	string	Specify the SHA value of an image.
filter	Optional	string	Filter the list by providing a query using Qualys syntax. Refer to the "How to Search" topic in the online help for assistance with creating your query.
pageNumber	Optional	integer	Specify the page to be returned. Page numbers start with 1.
pageSize	Optional	integer	Specify the number of records per page to be included in the response.

Sample: Fetch a List of Detected Malwares for an Image

API Request:

```
curl -X 'GET'
'<qualys_base_url>/csapi/v1.3/images/9287a1a2856378618469b0460cb295799ec9
9506c3d9697193fad51276235b7d/layers/malware?pageNumber=1&pageSize=50'
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
```

Response:

```
{
  "data": [
    {
      "layerHash":
"3c779f3ff212ad57ac3c4ba19cbf8e0104e50f27beb178a4e69df5c8e70ac988",
      "layerFileName": "layer.tar",
      "layerMimeType": "application/x-tar",
      "layerCreatedDate": "1689812682000",
```

```
      "layerFilesAnalyzed": 1,
      "layerMalwareCount": 1,
      "prediction": "malicious",
      "score": 1,
      "severity": 3,
      "category": "dropper",
      "family": "mirai",
      "createdBy": null
    },
    {
      "layerHash":
"994393dc58e7931862558d06e46aa2bb17487044f670f310dffe1d24e4d1eec7",
      "layerFileName": "layer.tar",
      "layerMimeType": "application/x-tar",
      "layerCreatedDate": "1689811077000",
      "layerFilesAnalyzed": 16,
      "layerMalwareCount": 0,
      "prediction": "unknown",
      "score": null,
      "severity": null,
      "category": null,
      "family": null,
      "createdBy": null
    }
  ],
  "count": 2,
  "groups": {}
}
```

Show Malware Files Detected for an Image Layer

API affected	/csapi/v1.3/images/{imageSha}/layers/{layerHash}/malware/files
Operator	GET
New or Updated APIs	New

Shows a list of malware files detected for a particular image layer.

Input Parameter

Parameter	Mandatory?	Data Type	Description
imageSha	Mandatory	string	Specify the SHA value of an image.
layerHash	Mandatory	string	Specify the hash value of a layer.

Sample: Show Malware Files Detected for an Image Layer

API Request:

```
curl -X 'GET'
'<qualys_base_url>/csapi/v1.3/images/9287a1a2856378618469b0460cb295799ec9
9506c3d9697193fad51276235b7d/layers/3c779f3ff212ad57ac3c4ba19cbf8e0104e50
f27beb178a4e69df5c8e70ac988/malware/files'
-H 'accept: application/json'
-H 'Authorization: Bearer'
```

Response:

```
{
  "data": [
    {
      "layerHash":
"3c779f3ff212ad57ac3c4ba19cbf8e0104e50f27beb178a4e69df5c8e70ac988",
      "fileHash":
"e684a0308c3a040f6a9f892eeae413676ed52bc45e3910a6ad4e4af78378b07d",
      "imageHash":
"9287a1a2856378618469b0460cb295799ec99506c3d9697193fad51276235b7d",
      "fileName": "libz.so.1",
      "fileType": "ELF",
      "createdDate": null,
      "fileSize": 0,
      "prediction": "malicious",
      "score": 1,
      "severity": 3,
      "category": "dropper",
      "family": "mirai",
```

```
      "mimeType": "application/x-executable"
    }
  ],
  "count": 1,
  "groups": null
}
```

Show Image Details with Malware, Secrets, and Compliance Information

API affected	/csapi/v1.3/images/{imageSha}
Operator	GET
New or Updated APIs	Updated

A new input parameter, scanDetails, in now available to specify the type of scan data to be fetched in the image details. You can specify "secrets", "malware", or "compliance" to fetch the secrets, malware, or compliance scan information for an image, respectively.

Input Parameter

Parameter	Mandatory?	Data Type	Description
scanDetails	Optional	string	Specify the type of scan details you want to fetch in the image details. The valid values are: - For malware information: malware - For secrets information: secrets - For compliance information: compliance You can specify multiple values separated by comma.

Sample: Fetch Malware and Secrets Information for an Image

API Request:

```
curl -X 'GET'
'<qualys_base_url>/csapi/v1.3/images/9287a1a2856378618469b0460cb295799ec9
9506c3d9697193fad51276235b7d?scanDetails=malware%2Csecrets' \
-H 'accept: application/json'
-H 'Authorization: Bearer <token>'
```

Response:

```
{
    "created": "1689754821000",
    "updated": "1689813088151",
    "author": "",
    "repo": [
        {
```

```
            "registry": "54.159.185.33:80",
            "tag": "404test",
            "repository": "malwaretestimage/qapods"
        }
    ],
    "repoDigests": [
        {
            "registry": "54.159.185.33:80",
            "digest":
"974557a02e976a11e5513b1486f82389ee8745dcbc3fa8023d0956bb9c4efa48",
            "repository": "malwaretestimage/qapods"
        }
    ],
    "label": null,
    "uuid": "21f9af9c-a7dd-31bd-b4b9-054a2e7a9825",
    "sha":
"9287a1a2856378618469b0460cb295799ec99506c3d9697193fad51276235b7d",
    "operatingSystem": "Alpine Linux 3.16.2",
   ...
    "malware": {
        "imageMalwareCount": 1,
        "malwarePrediction": {
            "prediction": "malicious",
            "score": 1,
            "severity": 3,
            "category": "dropper",
            "family": "mirai"
        }
    },
    "lastMalwareScanned": null,
    "exceptions": null,
    "secrets": [
        {
            "severity": "LOW",
            "filePath": "/root/foo/foo1.txt",
            "layerSha":
"7afaca6fd6f46466f2f23f51c647918c7818a431792547db3a7bc033d261a1e3",
            "match": null,
            "startLine": 0,
            "secretType": "Easypost API Token"
        },
        {
            "severity": "LOW",
            "filePath": "/root/foo/foo1.txt",
            "layerSha":
"7afaca6fd6f46466f2f23f51c647918c7818a431792547db3a7bc033d261a1e3",
            "match": null,
            "startLine": 0,
            "secretType": "Adobe Client ID (Oauth Web)"
```

```
        },
        {
            "severity": "MEDIUM",
            "filePath": "/root/foo/foo1.txt",
            "layerSha":
"7afaca6fd6f46466f2f23f51c647918c7818a431792547db3a7bc033d261a1e3",
            "match": null,
            "startLine": 0,
            "secretType": "Asana Client Secret"
        },
        {
            "severity": "CRITICAL",
            "filePath": "/home/qatest/key/gcp-service-account.json",
            "layerSha":
"5bc804df91a229c1f26d254b5247c699c1e1a53673ec1d30e263e7b4bda96beb",
            "match": null,
            "startLine": 0,
            "secretType": "Google (GCP) Service-account"
        }
    ...
    ],
    "softwares": [
        {
            "name": "libssl1.1",
            "version": "1.1.1q-r0",
            "scanType": "DYNAMIC",
            "packagePath": null,
            "fixVersion": "1.1.1u-r0",
            "vulnerabilities": [
    ...
            ]
        }
    ],
    "lastComplianceScanned": "1689813012500"
}
```

Fetch a List of Images (Bulk API)

API affected	/csapi/v1.3/images/list
Operator	GET
New or Updated APIs	Updated

A new input parameter, scanDetails, in now available to specify the type of scan data to be fetched. You can specify "secrets" or "malware" to fetch the secrets or malware scan information for an image, respectively.

Input Parameter

Parameter	Mandatory?	Data Type	Description
scanDetails	Optional	string	Specify the type of scan details you want to fetch. The valid values are: - For malware information: malware - For secrets information: secrets You can specify multiple values separated by comma.

Sample: Fetch a List of Images in your Account (with Malware Information)

API Request:

```
curl -X "GET"
"<qualys_base_url>/csapi/v1.3/images/list?limit=1&scanDetails=malware"
-H "accept: application/json"
-H "Authorization: Bearer <token>"
```

Response:

```
{
    "data": [
        {
            "created": "1683673870000",
            "updated": "1690897352513",
            "author": "",
            "repo": [
                {
                    "registry": null,
                    "tag": "alpine",
```

```
                    "repository": "test_scan_target"
                },
                {
                    "registry": null,
                    "tag": "latest",
                    "repository": "alpine"
                }
            ],
            "repoDigests": [
                {
                    "registry": null,
                    "digest":
"02bb6f428431fbc2809c5d1b41eab5a68350194fb508869a33cb1af4444c9b11",
                    "repository": "alpine"
                }
            ],
            "label": null,
            "uuid": "8f595428-d6f7-3961-ade8-ede516d47771",
            "sha":
"112b554c1c45d22c9d1aa836828828e320a26011b76c08631ac896cbc3629ed0",
            "operatingSystem": null,
            "customerUuid": "78ff6722-3d25-42b8-806d-8b710de88886",
            "dockerVersion": "20.10.23",
            "size": 7322585,
            "layers": [
                {
                    "size": "444",
                    "createdBy": "CMD [\"/bin/sh\"]",
                    "created": "1683673870000",
                    "comment": "",
                    "id": "5e2b554c1c45",
                    "sha":
"5e2b554c1c45d22c9d1aa836828828e320a26011b76c08631ac896cbc3625e3g",
                    "tags": [
                        "alpine:latest"
                    ]
                }
                ...
            ],
            "architecture": "amd64",
            "imageId": "112b554c1c45",
            "lastScanned": null,
            "registryUuid": null,
            "source": null,
            "users": null,
            "lastFoundOnHost": null,
            "isDockerHubOfficial": null,
            "isInstrumented": null,
            "instrumentedFrom": null,
```

```
            "instrumentationState": null,
            "scanType": null,
            "scanTypes": null,
            "softwares": null,
            "vulnerabilities": null,
            "malware": {
                "imageMalwareCount": 2,
                "malwarePrediction": {
                    "prediction": "malicious",
                    "score": null,
                    "severity": null,
                    "category": null,
                    "family": null
                }
            },
            "lastMalwareScanned": "1690897352455"
        }
    ],
    "limit": 1
}
```

Expiration Date for Reports

While creating a report, you can now set an expiration date for your report. The report is removed from your account after the specified date.

Furthermore, when fetching a list of reports available in your account, you can now see the expiry date for each report.

The following APIs have been updated:

Create a Report Request

Fetch a List of Reports

Create a Report Request

API affected	/csapi/v1.3/reports
Operator	POST
New or Updated APIs	Updated

You can now set an expiration date for your reports. The reports are removed from your account after the specified date.

Input Parameter

Parameter	Mandatory?	Data Type	Description
expireAfter	Mandatory	string	Specify a time period after which the report expires and gets deleted from your account. The valid values are (days): 1, 7, 30, or 90.

Sample: Create a Report Expiring After a Month

API Request:

```
curl -X "POST"
  "<qualys_base_url>/csapi/v1.3/reports"
  -H "accept: application/json"
  -H "Authorization: Bearer <token>
  -H "Content-Type: application/json"
  -d "{
  "description":"Demo Report","name":"My Container
Report","templateName":"CS_CONTAINER_VULNERABILITY",
"filter":"status:running","displayColumns":["containerid","uuid","qid"],
  "expireAfter": "30"
}"'
```

Response:

```
{
  "reportUuid": "7b972e20-2ef3-11ee-814b-3dadcc61dcfb"
}
```

Fetch a List of Reports

API affected	/csapi/v1.3/reports
Operator	GET
New or Updated APIs	Updated

A new parameter, expireAfter, is now available to show the time duration remaining before a report is deleted from your account.

Sample: List Reports Available in Your Account

API Request:

```
curl -X GET
"<qualys_base_url>/csapi/v1.3/reports?pageNumber=1&pageSize=50" --header
"Authorization: Bearer <token>"
```

Response:

```
{
  "data": [
    {
      "reportUuid": "1888e660-d238-11ed-9dcd-f52cd2719060",
      "createdAt": "2023-04-03T15:56:13.000Z",
      "reportName": "test1",
      "description": null,
      "fileFormat": "csv",
      "templateName": "CS_IMAGE_VULNERABILITY",
      "status": "COMPLETED",
      "isScheduled": 1,
      "filter": null,
      "displayColumns": [
        "imageId",
        "qid"
      ],
      "expireOn": "2024-05-17T15:56:13.000Z"
    },
    {
      "reportUuid": "1884a0a0-d238-11ed-9dcd-f52cd2719060",
      "createdAt": "2023-04-03T15:56:13.000Z",
      "reportName": "test2",
      "description": "test2",
      "fileFormat": "csv",
      "templateName": "CS_IMAGE_VULNERABILITY",
      "status": "COMPLETED",
      "isScheduled": 1,
      "filter": null,
```

```
      "displayColumns": [
        "imageId",
        "qid"
      ],
      "expireOn": "2024-05-17T15:56:13.000Z"
    }
  ],
  "count": 2
}
```