



# Mastering Risk with Qualys: The Elastic Journey

Qualys Security Conference London

Wed 27, 2024

# We build search solutions on a single stack

Search

Observability

Security

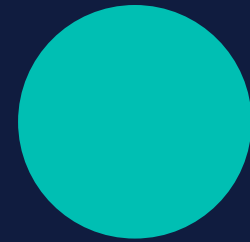


# Clément Fouque

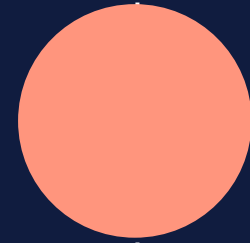
Vulnerability Management lead Elastic



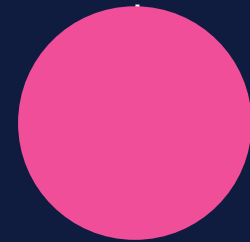
# Plan



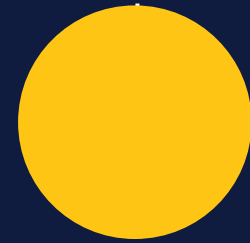
Environment



Asset Inventory

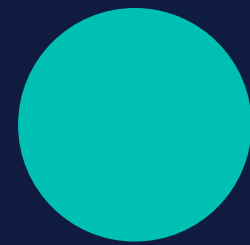


Vulnerability Management

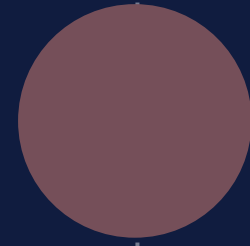


Evolutions

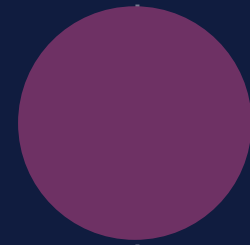
# Plan



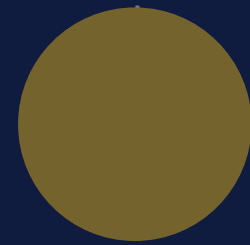
Environment



Asset Inventory



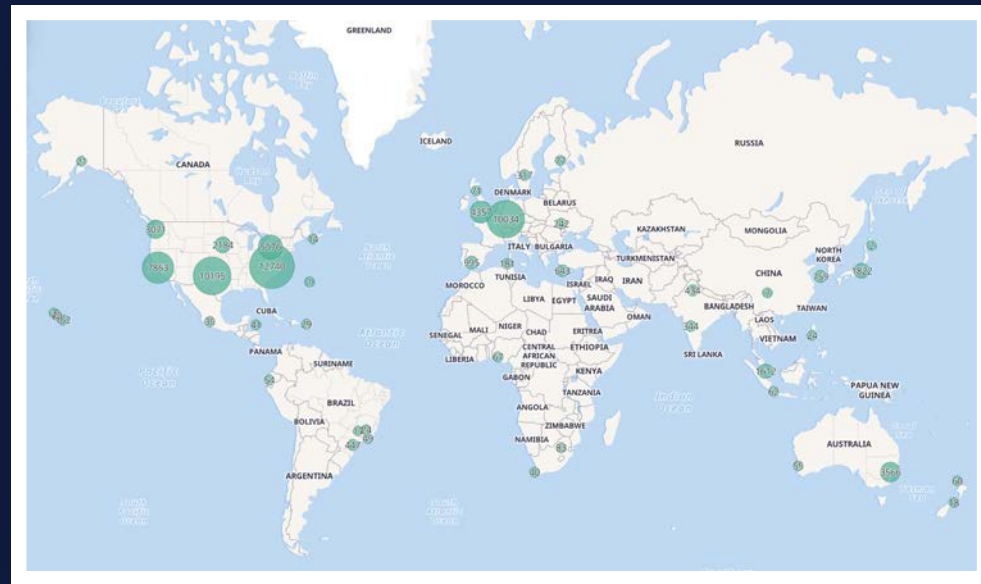
Vulnerability management



Evolutions

# Elastic InfoSec challenges

## Globally distributed workforce



~3,200

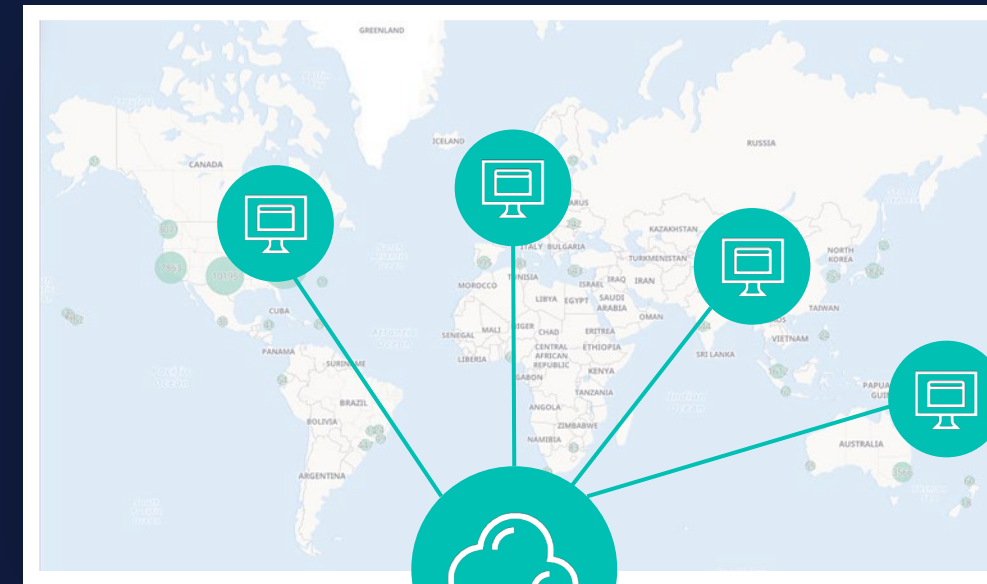
Elasticians



44

Countries

## Cloud native implementation



okta



# InfoSec by the numbers (daily)

150TB

## Security data

Enables us to monitor for abnormal and security relevant activity

600GB

## Endpoint data

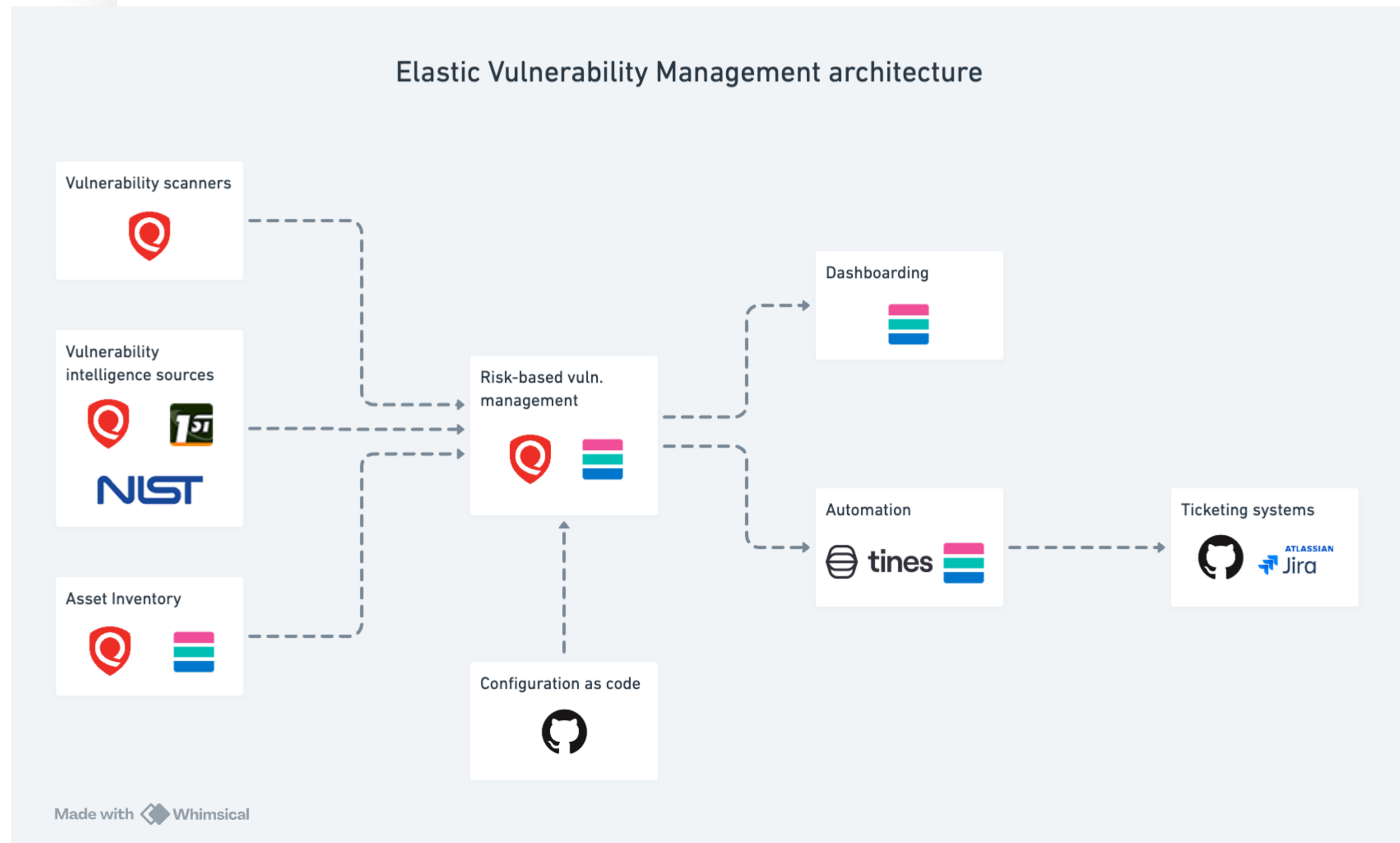
Amount of security data ingested daily from Elastic end user endpoints

>450K

## Endpoints

Globally dispersed cloud instances, virtual desktop environments, containers and user workstations

# Architecture







**1.2 FTE**

---

Architecture

Automatisation

Culture

- 40K Qualys agent
- 2K Policy Compliance
- 120+ connectors (15 TotalCloud)
- 5 container scanning
- 5 web applications scanning



# Cloud agents

Centralized management

Scan every 4 hours

No performance impact

Automatic update (agent and QIDs)

## Configuration Profile View

### View Mode

General Info >

Blackout Windows >

Performance >

Assign Hosts >

Agent Scan Merge

**VM Scan Interval**

PC Scan Interval

SCA Scan Interval

### Configure Scan Interval for Vulnerability Management

Configure the interval at which the agent collects data for Vulnerability Management for the assets associated with this profile.

**Data Collection Interval\*** 240 min (240 - 43200)

The time lapse between the completion of the previous scan and the start of the next scan

**Scan Delay\*** 0 min (0 - 720)

### Edit Mode

General Info >

Blackout Windows >

**Performance >**

Assign Hosts >

Agent Scan Merge >

### Configure Agent Performance

These settings govern how an agent behaves, from how often it checks in platform, to how often it checks the host for changes. It also includes performance control CPU and network utilization.

#### Performance

Select one of the performance levels below. Keep the default settings or customize them.

Based On: Low

## Configuration Profile Edit

Turn help tips: On | Off

### Edit Mode

**General Info >**

Blackout Windows >

Performance >

Assign Hosts >

Agent Scan Merge >

VM Scan Interval >

PC Scan Interval >

### Configure a profile for your agents

Customize agent behavior by defining a configuration profile. (\*) REQUIRED FIELD

#### Profile Name\*

ElasticCloud

Make this the default profile for the subscription

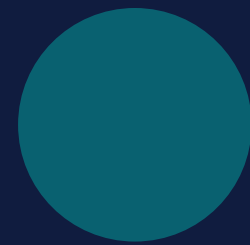
Suspend data collection for VM, PC, SCA and Inventory for all agents using this profile

In-Memory SQLite Databases

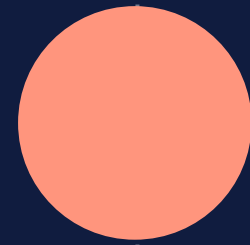
Prevent auto updating of the agent binaries

Enter a description for this configuration profile.

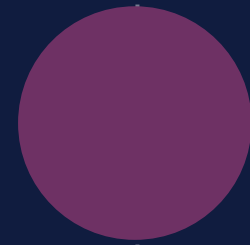
# Plan



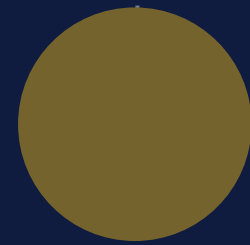
Environment



Asset Inventory



Vulnerability management



Evolutions



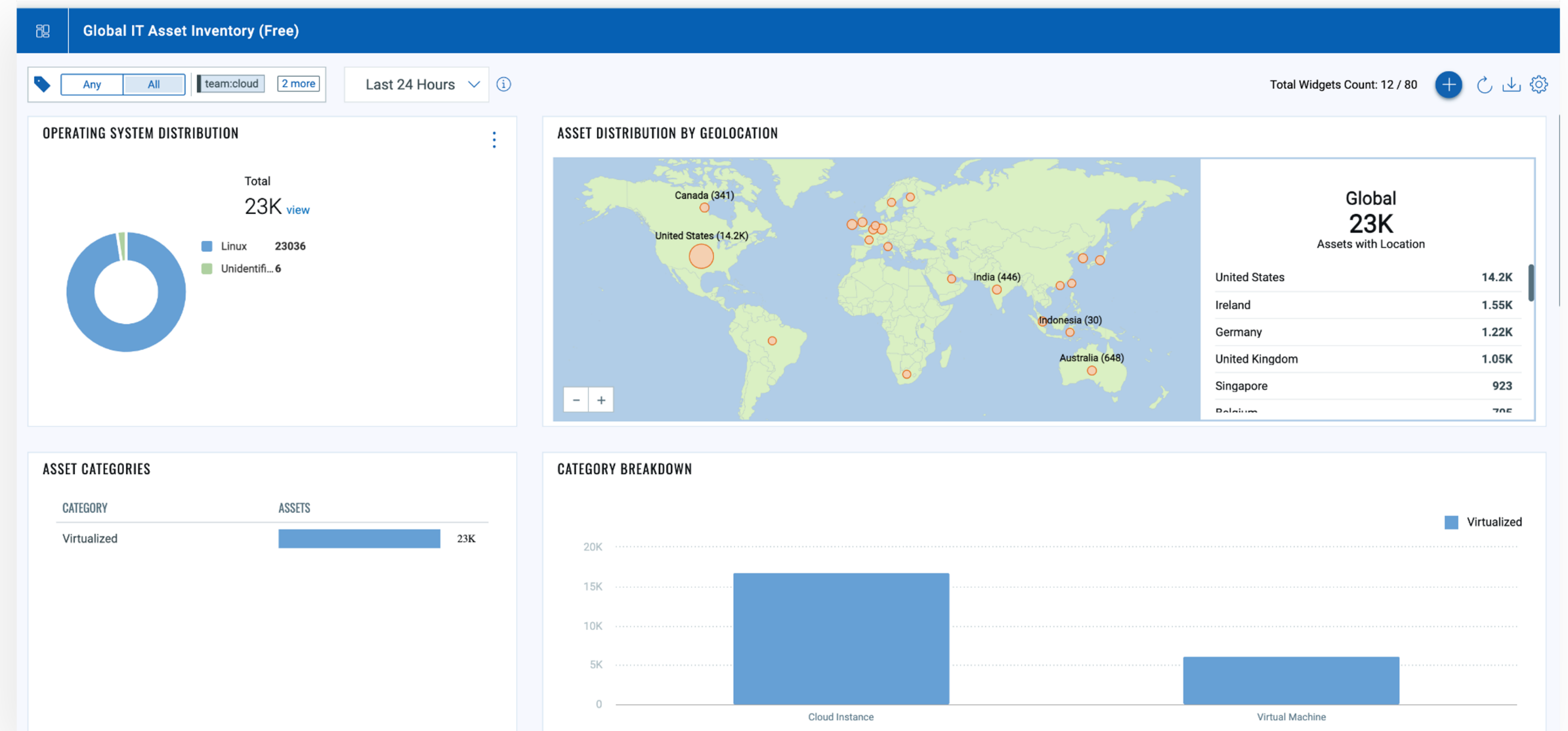
# Why and how have an asset inventory?

Free\*

Easy to implement

Automatic purge

Risk management





## Qualys tags

Enrichment

Parent/child relation

Access based on tags

Define criticality

API

NAME ↓

asset\_criticality:5

asset\_criticality:5

asset\_criticality:5

asset\_criticality:4

asset\_criticality:3

asset\_criticality:1

### Asset Criticality Score

This score represents the criticality of the asset to your business infrastructure.

**i** Here, score 1 being the lowest criticality and 5 being the highest criticality assigned to an asset.



```
{
  "ServiceRequest": {
    "data": {
      "Tag": {
        "id": 77439203,
        "description": "asset_criticality:3",
        "ruleType": "GROOVY",
        "ruleText": "return asset.hasAnyTags([\\"data_classification:internal\\", \\"data_classification:nan\\"]);",
        "criticalityScore": 3
      }
    }
  }
}
```



# Qualys cloud connectors

2 modes: inventory and compliance

API

← Connector Summary: InfoSec infosec AWS Connector - elastic-...

View Mode

- Connector Details
- Regions
- Tags & Activation
- Last Job Summary

## Tags & Activation

### Activation

Automatically activate all assets for:

**VM** **PC**

Zero-touch Cloud Perimeter Scan:  
Disabled

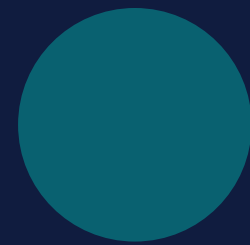
### Tags (6)

env:production:co... data\_classificati...  
owner:team:infose...

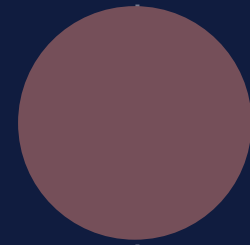
```
1  {
2    "ServiceRequest": {
3      "data": {
4        "AwsAssetDataConnector": {
5          "name": "InfoSec infosec AWS Connector",
6          "description": "Connector updated through API. Configur
7          "id": [REDACTED],
8          "defaultTags": {
9            "set": {
10             "TagSimple": [
11               {
12                 "id": 68075445,
13                 "name": "team:infosec:connector"
14               },
15               {
16                 "id": 68099223,
17                 "name": "env:production:connector"
18               },
19               {
20                 "id": 68448017,
21                 "name": "data_classification:internal"
22               },
23               {
24                 "id": 75214188,
25                 "name": "owner:division:engineering"
26               },

```

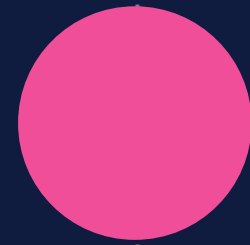
# Plan



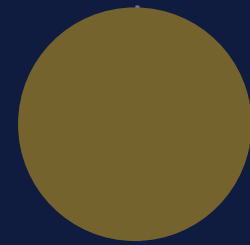
Environment



Asset Inventory



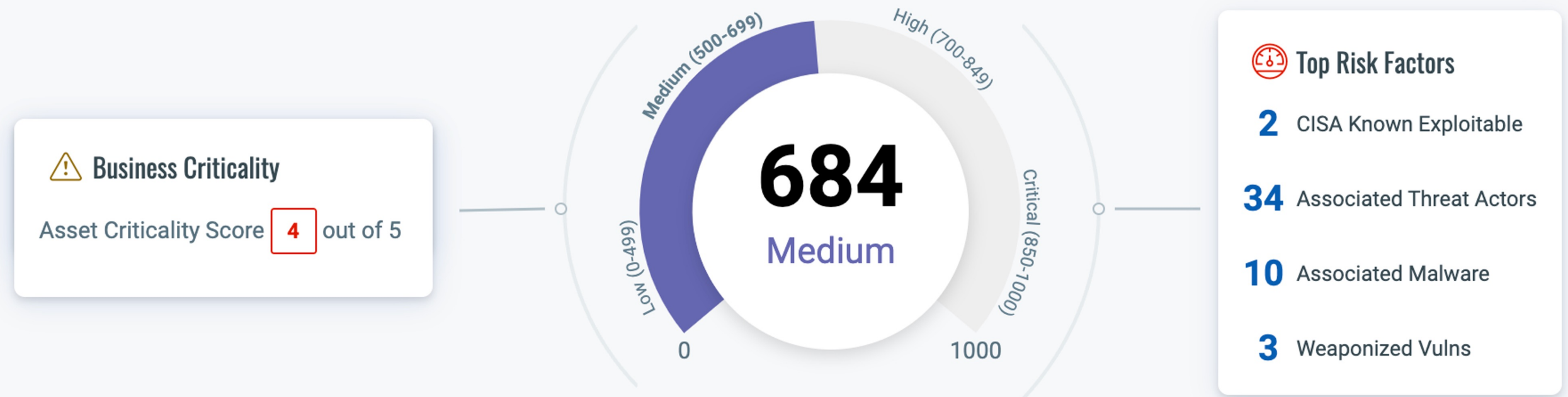
Vulnerability management



Evolutions



## TruRisk™ Score and its Contributing Factors



## Prioritisation

Qualys Detection Score

Asset Risk Score

NAME	CRITICALITY ⓘ	TruRisk™ Score ⓘ ↓	OPERATING SYSTEM	HARDWARE
i 1 C	57 3	4 650	⊗ Canonical Ubuntu Bionic B... 18.04 LTS 18.04.6 LTS	Amazon Web Servic... Amazon EC2 M5 m5... Cloud Instance
i 1 1	52 7	4 650	⊗ Canonical Ubuntu Bionic B... 18.04 LTS 18.04.6 LTS	Amazon Web Servic... Amazon EC2 M5 m5... Cloud Instance
i 1 C	5-98 75	3 504	⊗ Canonical Ubuntu Jammy ... 22.04 LTS 22.04.2 LTS	Xen Project HVM domU Virtual Machine





# Exception Management

Search list

Remediation policies

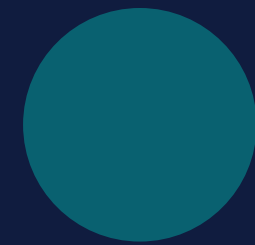
Tickets

API

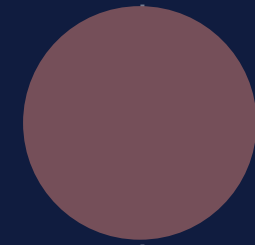
376157	Apache Log4j Remote Code Execution (RCE) Vulnerability (Log4Shell) Fixed Ignored	100
376178	Apache Log4j Remote Code Execution (RCE) Vulnerability (CVE-2021-45046) (Log4Shell) Fixed Ignored	100
376194	Apache Log4j Denial of Service (DoS) Vulnerability (CVE-2021-44228) (Log4Shell) Fixed Ignored	95
376209	Apache Log4j Remote Code Execution (RCE) Vulnerability (CVE-2021-44228) (Log4Shell) Fixed Ignored	95

```
{
  "id": [REDACTED],
  "name": "engineering_infosec_seceng",
  "qualys": {
    "tags": {
      "include": [
        "team:infosec"
      ],
      "exclude": [
      ]
    }
  },
  "elastic": {
    "owner": {
      "division": "engineering",
      "org": "infosec",
      "team": "seceng"
    }
  },
  "qids": [
    {
      "id": [REDACTED],
      "status": "closed",
      "risk_treatment": "false_positive",
      "title": "[REDACTED]",
      "reference": [
        "[REDACTED]"
      ],
      "reason": "[REDACTED]",
      "review_date": "2021-12-17"
    }
  ]
}
```

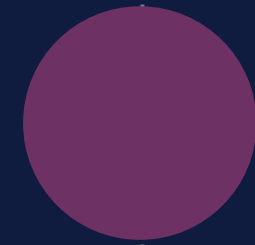
# Plan



Environment



Asset Inventory



Vulnerability management



Evolutions



# Container scanning Patch Management

Qualys Cloud Platform

Container Security

HOME DASHBOARD **ASSETS** POLICIES EVENTS REPORTS CONFIGURATIONS

Assets Hosts **Images** Containers Registries

768 Total Images

Search for images...

31 Images detected without ...

528 Images with Sev 5, 4 Vulne...

2 Docker Hub Official Images

53 Images not Compliant

REGISTRY

registry.redhat.io	567
docker.io	72
quay.io	65
registry-1.docker...	21
k8s.gcr.io	16
5 more	

VULNERABILITIES

Severity 5	281
Severity 4	4.88K
Severity 3	22K
Severity 2	4.13K
Severity 1	36

COMPLIANCE POSTURE

FAIL	96
PASS	10

Actions (0)

REGISTRY	REPOSITORY	CREATED ON ↓	TAGS ⓘ	IMAGE TAGS ⓘ
registry.redhat.io	<a href="#">redhat/redhat-operator-index</a> Image Id: 3a665de450ec	Jun 16, 2023	rte_test	v4.6
registry.redhat.io	<a href="#">redhat/redhat-operator-index</a> Image Id: c8061505d93e	Jun 15, 2023	-	v4.6
registry.redhat.io	<a href="#">redhat/redhat-operator-index</a> Image Id: 912f40d23052	Jun 15, 2023	-	v4.6
docker.io	<a href="#">nginx</a> Image Id: 55ba84d7d539	Jun 14, 2023	-	stable-alpine
registry.redhat.io	<a href="#">redhat/certified-operator-index</a> Image Id: 50b1bd5b162e	Jun 6, 2023	-	v4.6
registry.redhat.io	<a href="#">redhat/certified-operator-index</a> Image Id: 17076fbe42eb	May 31, 2023	-	v4.6
registry.redhat.io	<a href="#">redhat/redhat-operator-index</a> Image Id: cb2dbfae9ad8	May 31, 2023	-	v4.6
registry.redhat.io	<a href="#">redhat/redhat-operator-index</a> Image Id: 274df245abda	May 30, 2023	-	v4.6
registry.redhat.io	<a href="#">redhat/redhat-operator-index</a> Image Id: 1029823fa2b4	May 30, 2023	-	v4.6

# Master your risk with Qualys

1

## Asset Inventory

Tags  
Connectors

2

## TrueRisk

Qualys Detection Score  
Asset Risk Score

3

## Reporting

API