

# External Exposure



Every cloud resource that is exposed to the public internet represents a potential point of attack for malicious actors. Reduce this type of risk by minimizing the number of publicly exposed resources to only those that are absolutely required for business needs, and by actively monitoring for newly exposed resources.

- ✓ For tenants with a Wiz Dynamic Scanner, all the queries in the External Exposure Dashboard also verify the port status is not closed (i.e. `Port Status not equals Closed`). Tenants without an enabled Dynamic Scanner are unaffected.

The following scenarios provide step-by-step instructions to help you understand a few key ways we want you to use Wiz to address your External Exposure risks:

- [Find all exposed VMs, containers, serverless functions, buckets, and database servers](#)
- [Check whether a specific resource is exposed](#)
- [VMs and containers with wide exposure \(0.0.0.0/0\)](#)
- [Identify buckets with public read/write access](#)
- [Unpatched VMs with the most Critical/High severity Vulnerabilities](#)
- [All application endpoints that responded successfully to HTTP GET](#)
- [All application endpoints that expose interesting technologies](#)

For a more abstract discussion of exposure and answers to frequently asked questions, see the How Wiz Works page on [Network Exposure](#).




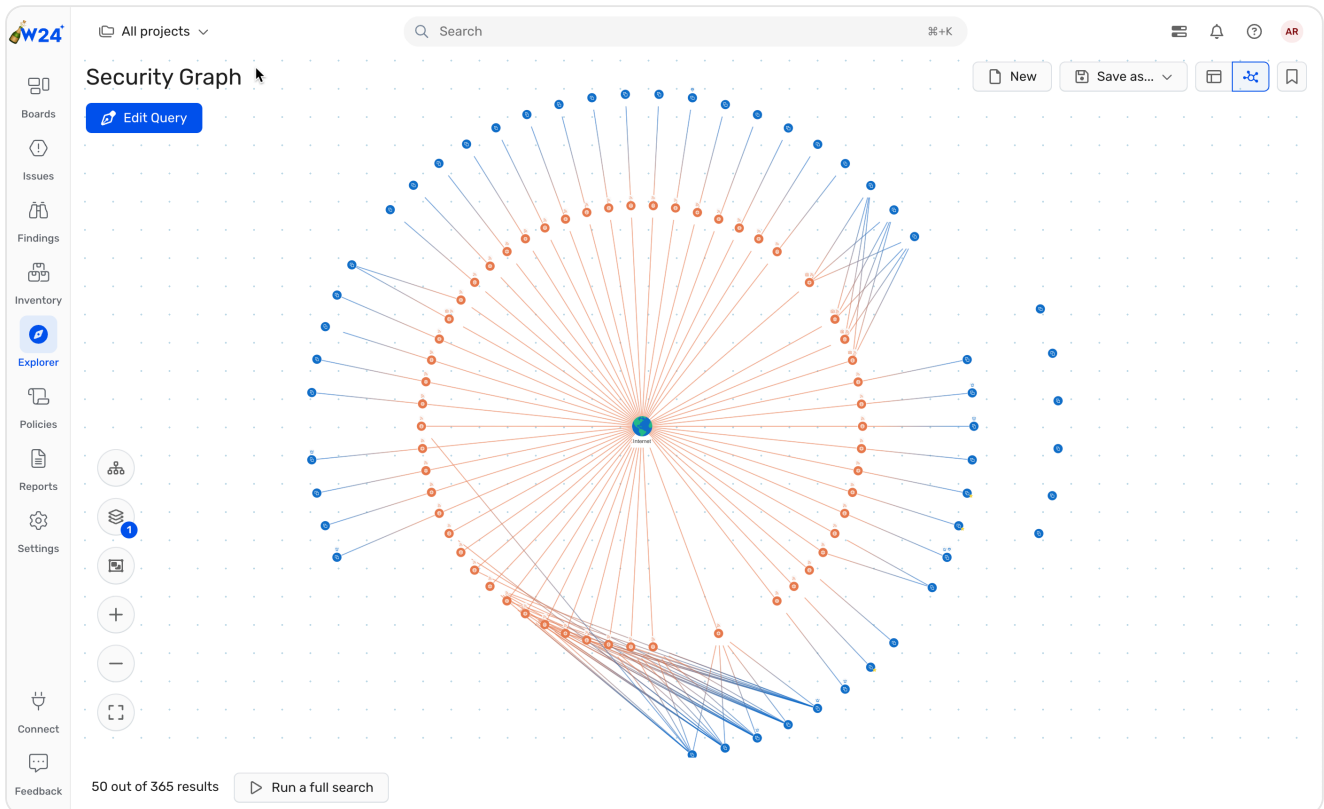
You can watch our webinar on [External Exposure](#).

## Find all exposed VMs, containers, serverless functions, buckets, and database servers


Wiz calculates effective exposure for many other cloud resources, but these five represent the some of the most common use cases for exposure.


To find exposed resources:

1. From the Security Graph, click Cloud Resource, and add "bucket", "container", "database server", "virtual machine", "serverless", and/or any other resource type whose exposure you want to investigate ([direct link](#)).
2. To the right of the "one of 5 options" criterion, click  > Internet exposure. The table of results lists all VMs, containers, serverless functions, buckets, and database servers for which Wiz has identified a path to the public internet.

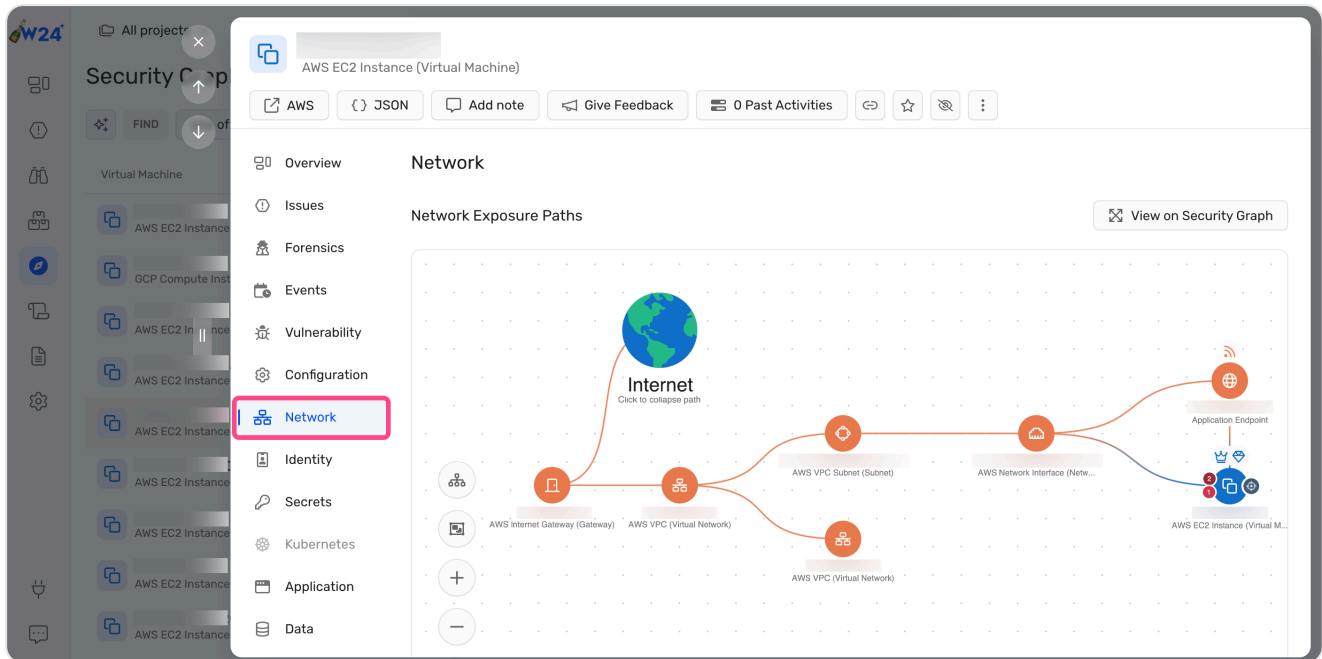


### 3. (Optional) Explore the results in graph view:

- Narrow down your search criteria.
- At the top right, click Graph View, or press .
- On the left, click Layers > Public Exposure.
- On the left, click Layouts repeatedly to cycle through different organizational schemes.

 A very broad query like VMs, containers, serverless functions, buckets, and database servers that are accessible from the internet could easily return thousands of results, but the Security Graph is optimized to show only 50 results at a time. Click Load More to add another 50 results to the current graph view, or narrow the query by removing resource types and/or adding filter criteria.

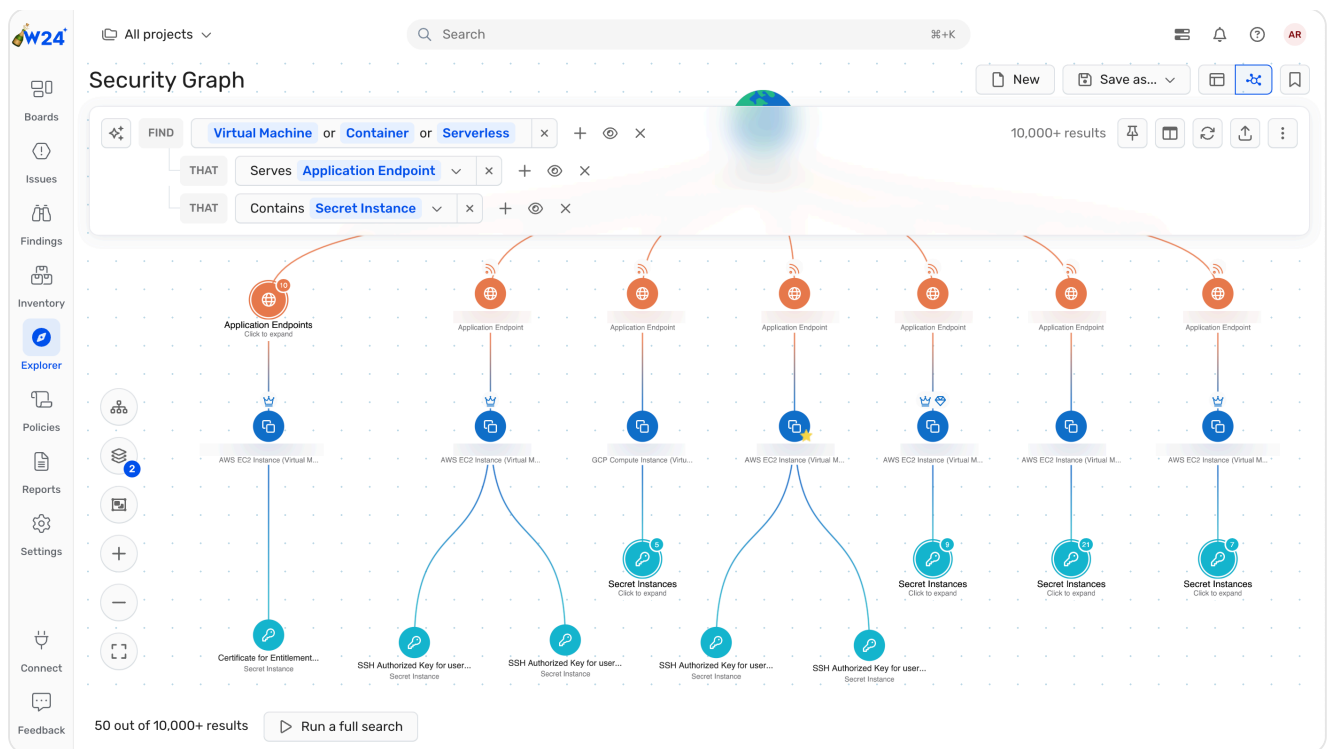
1. From the results of a query, click a resource name. Its details drawer opens on the right.



2. In the details drawer, switch to the Network tab. The resource's network exposure path is shown in a mini-Security Graph.
3. Scroll down in the Network tab to view related information, such as the resource's network addresses and network security groups along with other cloud resources in the same Vnet.

## VMs and containers with wide exposure (0.0.0.0/0)

1. From the Security Graph, search for VMs, containers, serverless functions with application endpoints ([sample query](#)).
2. Add filter criteria to gauge the potential damage if a malicious actor were able to reach these resources. The more types of risk are present, the greater the potential damage and the likelihood that someone will find their way in.



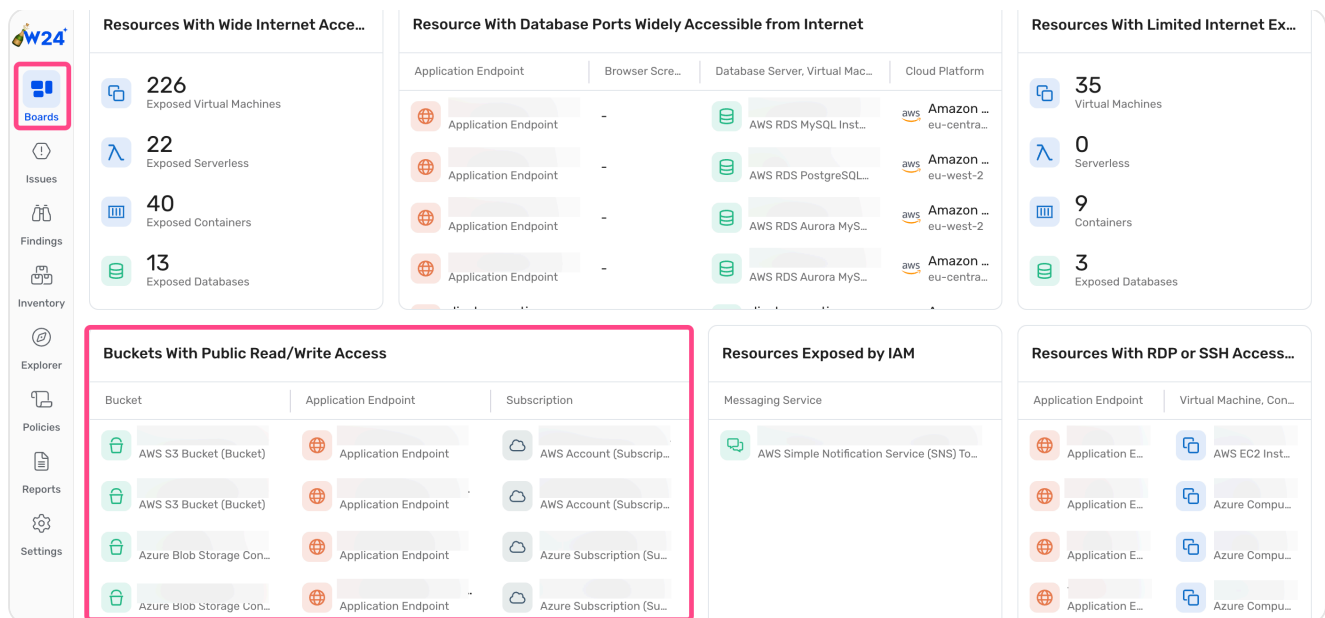
For instance:

- Are there secret instances on them? On the VM or Container criterion, click + > Secret Instance ([direct link](#)).
- Are there Configuration Findings associated with them? On the VM or Container criterion, click + > Configuration Finding ([direct link](#)).
- Do they have admin permissions? On the VM or Container criterion, click + > Admin Permissions ([direct link](#)).
- Do they have high permissions? On the VM or Container criterion, click + > High Permissions ([direct link](#)).

## Identify buckets with public read/write access

Buckets are often configured to be public by design in order to incorporate them in app backend and frontend flows. This approach sometimes causes the misconfiguration of bucket permissions by, for instance, exposing buckets to external write or making a bucket with confidential information available to the public.

1. Go to the External Exposure board.



2. Scroll down then click Buckets with Public Read/Write Access ([direct link](#)).
3. Review all buckets that allow external read/write. Verify that you are familiar with all of the identified resources and that these permissions were granted intentionally.
4. Click a bucket to check key info such as its region, whether it has logging enabled (recommended), etc.
5. Click the Network tab to see the bucket's public endpoint and test its visibility to external users.

## Unpatched VMs with the most Critical/High severity Vulnerabilities

1. Go to the External Exposure > Unpatched VMs Accessible From 0.0.0.0/0 widget.
2. On the workload criterion, click ☐ > Vulnerability that exists on it.
3. Click the new Has vulnerabilities query block. It expands to reveal its constituent Finding, Finding Type, and Vulnerability criteria. Click the Severity criterion, then de-select Medium and Low severity Findings. Only Critical and High severity Findings remain.
4. On the Application Endpoint criterion, click Column Visible > Hide these entities in order to make it possible to aggregate Findings per workload.
5. On the Finding criterion, click Column Visible > Aggregate these entities. The resulting bar graph shows which exposed workload is associated with the most Critical and High severity Vulnerabilities.

Consider prioritizing remediation efforts based on which exposed workloads are affected by the most Critical and High severity Vulnerabilities.

# All application endpoints that responded successfully to HTTP GET

Application endpoints with HTTP status 200 indicate you have an open successful connection which should be inspected.

1. From the Security Graph, click Cloud Resource and type Application Endpoint.
2. Click + and type Port Status equals Open. Hit Enter.
3. Click + and type HTTP Status Code equals 200. Hit Enter.
4. Browse the results of the final query ([direct link](#)).

---

# All application endpoints that expose interesting technologies

Locate all the actively open ports to technologies which you want to deny access to, such as Jenkins in this example. You add more technologies as you wish!

1. On the Security Graph, build the following query to detect Application Endpoints detected on a container or VM with an Open port status ([direct link](#)).
2. Click + and type Hosted Technology.
3. Click + and type Name. Select Starts with in the logical operator drop-down list and type the name of the technology you are interested in, such as Jenkins. For HTTPs ports, Wiz Dynamic Scanner includes a [validation screenshot](#).

---

 Updated 6 months ago

---

← Attack simulation for Cloud  
Detection and Response

Malware Detection →

Did this page help you?  **Yes**  **No**

English ▲