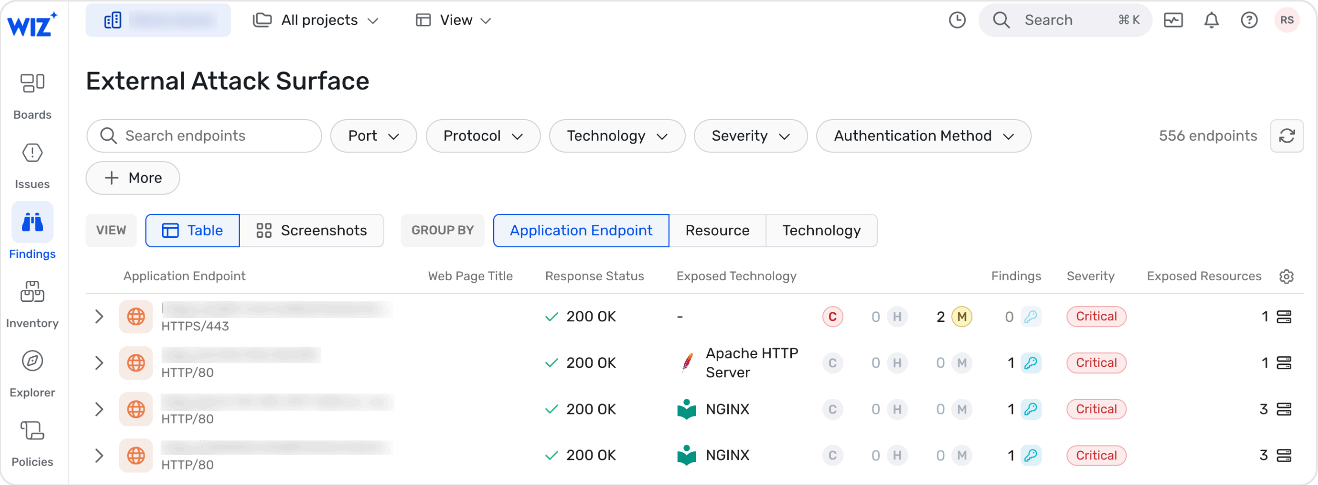
External Attack Surface

This is a preview feature that requires a Wiz Advanced license. Learn more about preview features and Wiz licenses.

The External Attack Surface page summarizes the scan results of the Dynamic Scanner regarding Application Endpoints detected by the network analyzer. It includes details such as web page titles, browser screenshots, exposed resources and technologies, and associated Findings. Learn about the Dynamic Scanner.



External Attack Surface

Search endpoints | Port | Protocol | Technology | Severity | Authentication Method | 556 endpoints

+ More

VIEW: Table | Screenshots — GROUP BY: Application Endpoint | Resource | Technology

Application Endpoint	Web Page Title	Response Status	Exposed Technology	Findings	Severity	Exposed Resources
[redacted] HTTPS/443		✓ 200 OK	-	C 0 H 2 M 0	Critical	1
[redacted] HTTP/80		✓ 200 OK	Apache HTTP Server	C 0 H 0 M 1	Critical	1
[redacted] HTTP/80		✓ 200 OK	NGINX	C 0 H 0 M 1	Critical	3
[redacted] HTTP/80		✓ 200 OK	NGINX	C 0 H 0 M 1	Critical	3

From the Findings > External Attack Surface page, you can:

- Filter findings
- View browser screenshots of all Application Endpoints
- Investigate an Application Endpoint
- Inspect all exposed technologies

Filter findings

To filter findings, apply one or more criteria:

- At the top left, type an Application Endpoint name in the search bar (e.g., 18.118.143.220:22).
- At the top, click Port, Protocol, Technology, etc. Then, select criteria to apply one or more filters. Once done, click Reset to remove all filters.

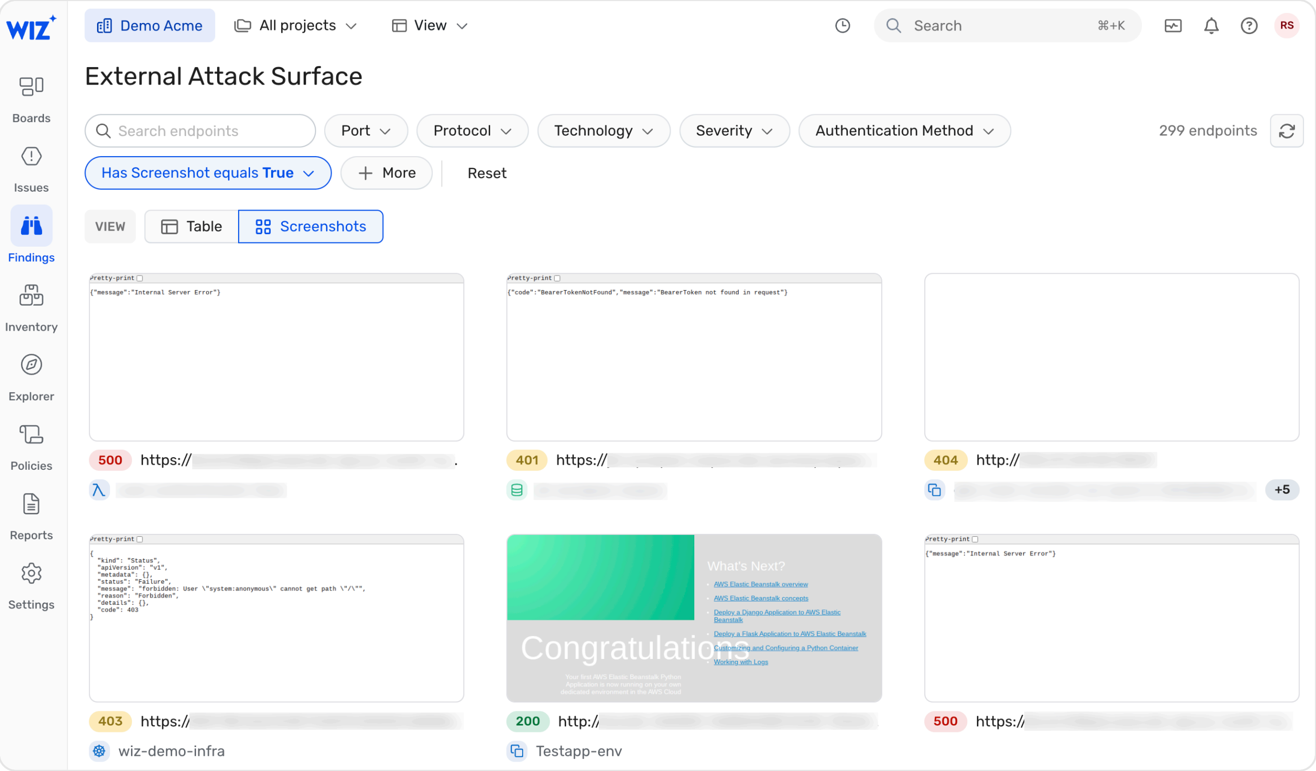
- At the top, click More and choose a filter to add it. You can add multiple filters.

View browser screenshots of all Application Endpoints

The Dynamic Scanner takes a screenshot of the browser when connecting to Application Endpoints. Learn more about validation screenshots.

To view browser screenshots:

1. Go to the Findings > External Attack Surface page.
2. At the top, click Screenshots.



```
{"message":"Internal Server Error"}
```

```
{"code":"BearerTokenNotFound","message":"BearerToken not found in request"}
```

```
{
  "kind": "Status",
  "apiVersion": "v1",
  "metadata": {},
  "status": "Failure",
  "message": "forbidden: User \"system:anonymous\" cannot get path \"/\"",
  "reason": "Forbidden",
  "details": {},
  "code": 403
}
```

```
{"message":"Internal Server Error"}
```

Investigate an Application Endpoint

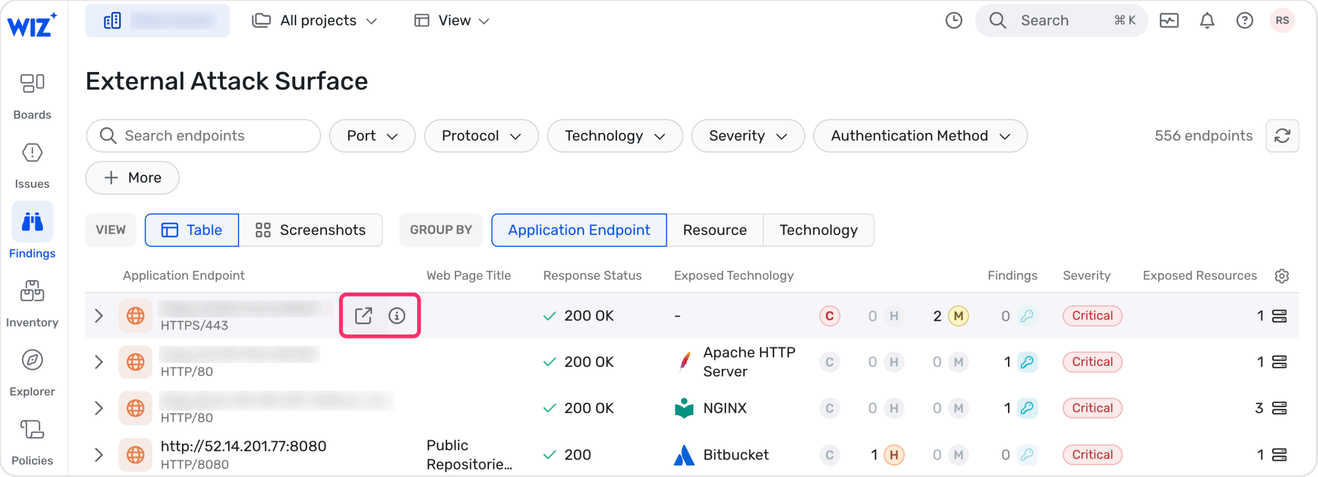
> Application Endpoints are ordered according to the severity and quantity of their associated Findings (i.e. Host Configuration Findings, Data Findings, and Secret Findings), with Secret Findings being always of critical severity. For example, an Application Endpoint with 1 Secret Finding will appear before an Application Endpoint with 5 high severity Data Findings.

To investigate an Application Endpoint:

1. Go to the Findings > External Attack Surface page.
2. At the top, group by Application Endpoint.
3. Choose an Application Endpoint and inspect its scan results (e.g., web pa response status, severity). You can also open the details drawer of an Application

English ▲

Endpoint by clicking ⓘ or visit the webpage for HTTP Application Endpoints by clicking ↗.



External Attack Surface

Application Endpoint	Web Page Title	Response Status	Exposed Technology	Findings				Severity	Exposed Resources
[redacted] HTTPS/443 ↗ ⓘ		✓ 200 OK	-	C	0 H	2 M	0 🔑	Critical	1
[redacted] HTTP/80		✓ 200 OK	Apache HTTP Server	C	0 H	0 M	1 🔑	Critical	1
[redacted] HTTP/80		✓ 200 OK	NGINX	C	0 H	0 M	1 🔑	Critical	3
http://52.14.201.77:8080 HTTP/8080	Public Repositorie...	✓ 200	Bitbucket	C	1 H	0 M	0 🔑	Critical	1

4. (Optional) Investigate the associated exposed resources:
   i. Click ❯ next to the Application Endpoint.
   ii. Choose an exposed resource and view important information about it at a glance (open Issues, locations, and associated Projects). Then, click it to open its details drawer.
   iii. At the top, click Validated Public Network Exposure to view the network exposure paths plotted on the Security Graph.

Inspect all exposed technologies

To inspect all exposed technologies:

1. Go to the Findings > External Attack Surface page.
2. At the top, group by Technology.
3. Choose a technology and view the findings (e.g., type, associated Application Endpoints).
4. Click the technology. Its details drawer opens to the right for further investigation.

Updated 23 days ago

← Network Exposure

CI/CD Scans →