Application layer attacks

- List of endpoints
  - Timeseries
    - Example: Hourly mitigation requests by product
  - Summary
    - Example: Mitigation requests by product
  - Top
    - Example: Top target locations
    - Example: Top attacks
- Next steps

While in HTTP requests you can examine all kinds of web requests, in application layer attacks you have access only to mitigated HTTP requests. These requests can be mitigated by one of several Cloudflare products, like WAF, Cloudflare DDoS Protection, Cloudflare bot solutions and others.

:::note[Mitigated traffic]

Mitigated traffic is any HTTP request from an end-user that has a terminating action applied by the Cloudflare platform. These include actions like `BLOCK` or challenges. :::

Since we are examining attacks, we can inspect both sides of an attack — both the source location and the target location of the attack. For the source of the attack Cloudflare uses the location the attack is coming from associated with the IP (note that the human orchestrator of the attack may be in a different location than the computer the attack is originating from). For the target location of the attacks, Cloudflare uses the billing location associated with the zone under attack.

This ability to filter by both sides of the attack is only available in the `top locations` endpoints. Unless otherwise specified, other endpoints are filtered by source location, like the origin location of the attack.

The magnitude of the attack is defined by the total number of mitigated requests.

Like in HTTP requests, these endpoints can be split into the ability to fetch a timeseries, a single value summarizing the entire date range, and a list of top locations.

List of endpoints

Timeseries

Example: Hourly mitigation requests by product

Let us examine the global distribution of mitigated requests by product.

```
curl
"https://api.cloudflare.com/client/v4/radar/attacks/layer7/timeseries_groups/mitigation_produc
t?aggInterval=1h&dateRange=1d&name=attacks&format=json" \
--header "Authorization: Bearer <API_TOKEN>"
```

From the abbreviated response below, we can conclude that distributed denial-of-service (DDoS) attacks make up the majority of the requests — which makes sense since DDoS attacks, by their very nature, will perform more requests. This is followed by WAF and then I reputation requests.

```
{
  "success": true,
  "errors": [],
  "result": {
    "attacks": {
      "timestamps": ["2022-11-05T11:00:00Z", ".."],
      "ddos": ["53.824302", "54.305823",  ".."],
      "waf": ["39.760956", "39.31228",  ".."],
      "ip_reputation": ["5.623487", "5.485468",  ".."],
      "access_rules": ["0.648368", "0.676456",  ".."],
      "bot_management": ["0.139733", "0.217155",  ".."],
      "api_shield": ["0.003154", "0.002819",  ".."],
      "data_loss_prevention": ["0.0", "0.0",  ".."]
    },
    "meta": {
      "dateRange": {
        "startTime": "2022-11-05T11:00:00Z",
        "endTime": "2022-11-06T11:00:00Z"
      },
□□□// ...
    }
```

```
  }
}
```

For more information refer to Get layer 7 attacks by mitigation technique, over time.

Summary

Example: Mitigation requests by product

We can also filter by source location and examine attacks coming from a specific place - in the following example, we examine attacks coming from Great Britain:

```
curl
"https://api.cloudflare.com/client/v4/radar/attacks/layer7/summary?location=GB&name=attacks_gb
&aggInterval=1h&dateRange=1d&format=json" \
--header "Authorization: Bearer <API_TOKEN>"
```


```
{
  "success": true,
  "errors": [],
  "result": {
□□"attacks_gb": {
□□□"waf": "75.012138",
□□□"ddos": "18.539149",
□□□"ip_reputation": "5.721021",
□□□"access_rules": "0.592515",
□□□"bot_management": "0.131998",
□□□"api_shield": "0.003178",
□□□"data_loss_prevention": "0.0"
  □},
□□"meta": {
□□□// ...
    }
□}
}
```


This response means that 75% of all mitigated requests coming from Great Britain were mitigated by the WAF product.

For more information refer to Get layer 7 attacks summary.

Top

Example: Top target locations

In the following example, we will examine the top locations being targeted in application layer attacks, in the last 24 hours:

```
curl
"https://api.cloudflare.com/client/v4/radar/attacks/layer7/top/locations/target?name=attacks_t
arget&limit=5&dateRange=1d&format=json" \
--header "Authorization: Bearer <API_TOKEN>"
```


```
{
  "success": true,
  "errors": [],
  "result": {
    "attacks_target": [
□□□{
□□□□"targetCountryName": "Belgium",
□□□□"targetCountryAlpha2": "BE",
□□□□"value": "18.536740",
□□□□"rank": 1
□□□},
□□□{
□□□□"targetCountryName": "United States",
□□□□"targetCountryAlpha2": "US",
□□□□"value": "16.116210",
□□□□"rank": 2
□□□},
□□□{
□□□□"targetCountryName": "China",
□□□□"targetCountryAlpha2": "CN",
□□□□"value": "13.864696",
□□□□"rank": 3
□□□},
□□□{
□□□□"targetCountryName": "India",
```

```
        "targetCountryAlpha2": "IN",
        "value": "4.344139",
        "rank": 4
      },
      {
        "targetCountryName": "Germany",
        "targetCountryAlpha2": "DE",
        "value": "4.182777",
        "rank": 5
      }
    ],
    "meta": {
      "dateRange": {
        "startTime": "2022-11-05T12:00:00Z",
        "endTime": "2022-11-06T12:00:00Z"
      },
      // ...
    }
  }
}
```


During the specified date range, mitigation requests to zones with a billing address located in Belgium represent 18%.

For more information refer to Get layer 7 top target locations.

Example: Top attacks

Which source-target location pairs constitute the biggest attacks in the last 24 hours?

```
curl
"https://api.cloudflare.com/client/v4/radar/attacks/layer7/top/attacks?limit=5&dateRange=1d&fo
rmat=json" \
--header "Authorization: Bearer <API_TOKEN>"
```

A typical response will be similar to the following:


```
{
  "success": true,
  "errors": [],
  "result": {
```

```
  "top_0": [
    {
      "originCountryName": "United States",
      "originCountryAlpha2": "US",
      "targetCountryName": "United States",
      "targetCountryAlpha2": "US",
      "value": "3.790724",
      "rank": 1
    },
    {
      "originCountryName": "United States",
      "originCountryAlpha2": "US",
      "targetCountryName": "Belgium",
      "targetCountryAlpha2": "BE",
      "value": "3.602177",
      "rank": 2
    },
    {
      "originCountryName": "China",
      "originCountryAlpha2": "CN",
      "targetCountryName": "Netherlands",
      "targetCountryAlpha2": "NL",
      "value": "3.017341",
      "rank": 3
    },
    {
      "originCountryName": "China",
      "originCountryAlpha2": "CN",
      "targetCountryName": "China",
      "targetCountryAlpha2": "CN",
      "value": "2.472068",
      "rank": 4
    },
    {
      "originCountryName": "Indonesia",
      "originCountryAlpha2": "ID",
      "targetCountryName": "China",
      "targetCountryAlpha2": "CN",
      "value": "2.056729",
      "rank": 5
```

```
□□□}
□□],
    "meta": {
□□□// ...
    }
  }
}
```


This means that 3.79% of all mitigated requests are from and to the US, 3.6% of all mitigated requests are from the US to Belgium, etc..

For more information refer to Get layer 7 top attack pairs.

Next steps

Refer to Network layer attacks for more information on data on layer 3 of the Open Systems Interconnection (OSI) model.

□□□ #2
□ □□□ □□□ 2026-11-01 03:12:00 UTC
□ □□□ □□□ 2026-11-01 03:12:02 UTC