Perimeter Overview

Published: 2024-02-05

The Perimeter Overview displays charts and interactive visualizations that help you monitor traffic that is entering and leaving your network through connections with external endpoints.

Perimeter Traffic

The Perimeter Traffic charts provide an overview of device traffic with external connections.

Inbound Traffic

This count shows the total amount of inbound traffic during the selected time interval. Click the count to view the rate that data is moving inbound from external endpoints and drill down by site or conversation.

Outbound Traffic

This count shows the total amount of outbound traffic during the selected time interval. Click the count to view the rate that data is moving outbound to external endpoints and drill down by site or conversation.

Devices Accepting Inbound Connections

This count displays the number of devices that accepted inbound connections from external endpoints during the selected time interval. Click the count to open a device group overview page that displays a list of devices, traffic data, and protocol activity.

Inbound Connections

This count displays the number of inbound connections that were initiated by external endpoints. Click the count to open a detailed view of these conversations.

Suspicious Inbound Connections

This count chart displays the number of connections that were initiated by suspicious external endpoints. ExtraHop identifies suspicious endpoints through threat intelligence data. Click the chart to open a filtered view of these conversations.

Suspicious Outbound Connections

This count displays the number of connections that internal endpoints initiated with suspicious external endpoints. ExtraHop identifies suspicious endpoints through threat intelligence data. Click the chart to open a filtered view of these conversations.

Uncommon Connections

(Reveal(x) 360 only) This count displays the number of outbound connections from your network to IP addresses that are not normally visited or have not been visited in the past. Click the chart to open a filtered view of these conversations.

Halo visualization

The halo visualization provides two views of your network connections to external endpoints: Cloud Services and Large Uploads.

External endpoints appear on the outer ring with connections to internal endpoints and appear as circles in the middle of the visualization. These visualizations enable you to prioritize your investigation for connections marked with high-risk detections or for high value devices.

To help identify high-traffic endpoints, inner circles and outer rings increase in size as traffic volume increases. In some cases, the size of inner circles and outer ring segments might be increased for readability. Click an endpoint to display precise traffic information.

Click **Cloud Services** to view connections between internal endpoints and cloud service providers. Cloud service providers and the amount of sent or received data appear in the information panel to the right. You can toggle between views that show **Bytes Out** to providers and **Bytes In** to your network.

Click **Large Uploads** to view connections between internal and external endpoints where over 1 MB of data was transferred in a single transmission out of your network to an external endpoint. External endpoints and the amount of uploaded data appear in the information panel to the right.

Here are some ways that you can interact with these halo visualizations:

- Hover over endpoints or connections to view available hostnames and IP addresses.
- Hover over endpoints or connections to highlight corresponding list items to the right. Likewise, hover over list items to highlight corresponding endpoints and connections in the halo visualization.
- Click endpoints or connections in the halo visualization to hold focus and display precise traffic information and links for your selection to the right.
- Click an external endpoint in the halo visualization or list to view the total amount of inbound or outbound traffic associated with the endpoint and connected internal endpoints.
- Click an internal endpoint in the list to view device properties and access links to associated information such as detections, records, or packets.
- Click the magnifying glass next to an endpoint in the list to view records associated with the endpoint.
- At the bottom of the list for cloud services, toggle between views that show Bytes Out and Bytes In to your network.
- Adjust the time interval to view connections at specified times, such as unexpected activity during evenings or weekends.

Map visualization

The Geolocation tab provides a world map of traffic between internal endpoints and geographic locations, which are highlighted in a contrasting color on the map. The intensity of the contrasting color represents the amount of traffic at that geolocation. Geolocations represented on the map are also listed in the right pane.

Click a highlighted geolocation from the map or the list to view the total amount of inbound or outbound traffic associated with connected internal endpoints.

Here are some ways that you can interact with the geolocation details and the map visualization:

- Click an internal endpoint in the list to view device properties and access links to associated information such as detections, records, or packets.
- Click the magnifying glass next to an endpoint in the list to view records associated with the endpoint.
- At the bottom of the list, toggle between views that show Bytes Out and Bytes In to your network.
- Click the controls located in the bottom right corner of the map to zoom in and out or return the map to the original position, or you can rotate your mouse wheel.
- Click and drag your mouse on the map or press the arrow keys on your keyboard to reposition the map view.
- Adjust the time interval to view traffic at specified times, such as unexpected activity during evenings or weekends.

Site selector and executive report

You can specify the sites you want to view data from on this page. Users with NDR module access can generate an executive report to share results.

Site Selector

Click the site selector at the top of the page to view data for one or more sites in your environment. View combined traffic across your networks or focus on a single site to help you quickly find device

data. The site selector indicates when all or some sites are offline. Because data is not available from offline sites, the charts and device pages associated with offline sites might not show data or might only show limited data. The site selector is only available from a console.

(NDR module only) Executive Report

Click **Generate Executive Report** to create a PDF file. The Executive Report provides a summary of the top detections and risks to your network from the last week. The Executive Report only includes information for the selected sites.