Perimeter Overview

Published: 2022-09-17

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.

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.

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.

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 chart 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.

Total External Traffic

This chart shows the rate that data is moving outbound and inbound from connections with external endpoints. Click the Inbound Traffic or Outbound Traffic data label to access menu options to create a new chart, search for related records, or drill down by conversation.

Halo visualization

The halo visualization provides three views of your network connections to external endpoints: Cloud Services, Countries, 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 **Countries** to view connections between internal endpoints and countries. The connections are broken down by the geographic location of the external endpoint. Countries 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 countries 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.
- Click endpoints or connections to hold focus and display precise traffic information and links for your selection in the information panel to the right.
- Click or hover an internal endpoint in the information panel to view device properties and access links to associated information such as detections, records, or packets.
- Adjust the time interval to view connections at specified times, such as unexpected activity during evenings or weekends.