Perimeter Overview

Published: 2020-06-17

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.

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.

Internal Endpoints Accepting Inbound Connections

This count chart displays the number of internal endpoints that accepted inbound connections from external endpoints during the selected time interval. Click the chart to open a filtered 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: Large Data Upload, Uncommon Destinations, and Cloud Service Traffic.

External endpoints are displayed in the outer ring with connections to internal endpoints, which are displayed 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 critical assets.

Click **Large Data Upload** to view connections where a large amount of data (25 MB or more) was transferred out of your network to an external endpoint in a single transmission.

Click **Uncommon Destinations** to view connections to uncommon or unknown endpoints.

Click **Cloud Service Traffic** to view connections to cloud service providers. You can toggle between views that show **Bytes Out** to providers and **Bytes In** to your network.

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

- Hover over endpoints or connections to view hostnames and IP addresses.
- Click endpoints or connections to hold focus and display information and links for your selection in an information panel to the right.
- Adjust the time interval to view connections at specified times, such as unexpected activity during evenings or weekends.