MANAGE GAUGES

Before working with the gauges, you must verify the prevention configuration option for your security technologies has been configured. Otherwise, prevented Actions will not be related to a security technology and will instead be included in the Unknown Security Technology category.

By default, the Gauges pull information for all dates and zones in the system, and display Malicious File Transfer, Data Exfiltration, Authentication & Authorization, and Command & Control Communications. You can configure this to include the dimensions, zones, and time range you are interested in.

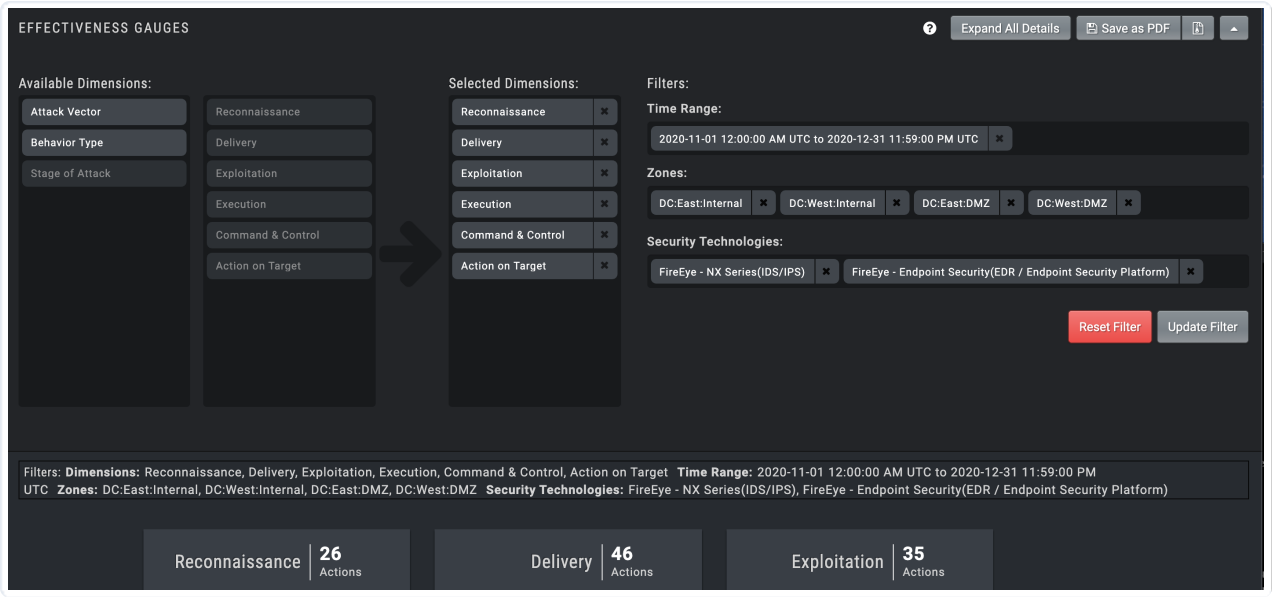
Each time you update the filters there is a small pause while the data is being pulled to redraw the Gauges. You see a scrolling bar in each Gauge to indicate the data is loading. The more Jobs included in a search, the longer it takes for the Gauges to load; if it is taking too long, adjust the time range and click **Update Filter** to cancel the previous query and start a new one.

If you configure your filter, this new configuration becomes the default when you use the same browser; **Reset Filter** returns the filter to the default dimensions, include all dates and zones, and automatically reloads the gauges.

Add a filter

1. Click **Expand**.
2. Select or remove Dimensions.
   - Select a Dimension category and then select the specific dimension you want - it automatically moves into the Selected Dimensions area.
   - Click the x next to a Dimension listed in the Selected Dimensions area to remove it from the filter.
3. To change the Time Range, Zones, or Security Technologies, click in the field and select one or more of the available options.
   If there is a defined time range already, you must delete it first before changing to a new one

   When you use the Zones filter, results include all Actions that match the destination Actor.
4. Click **Update Filter**.



Gauge Filter options

Export the Gauges and Gauge Details

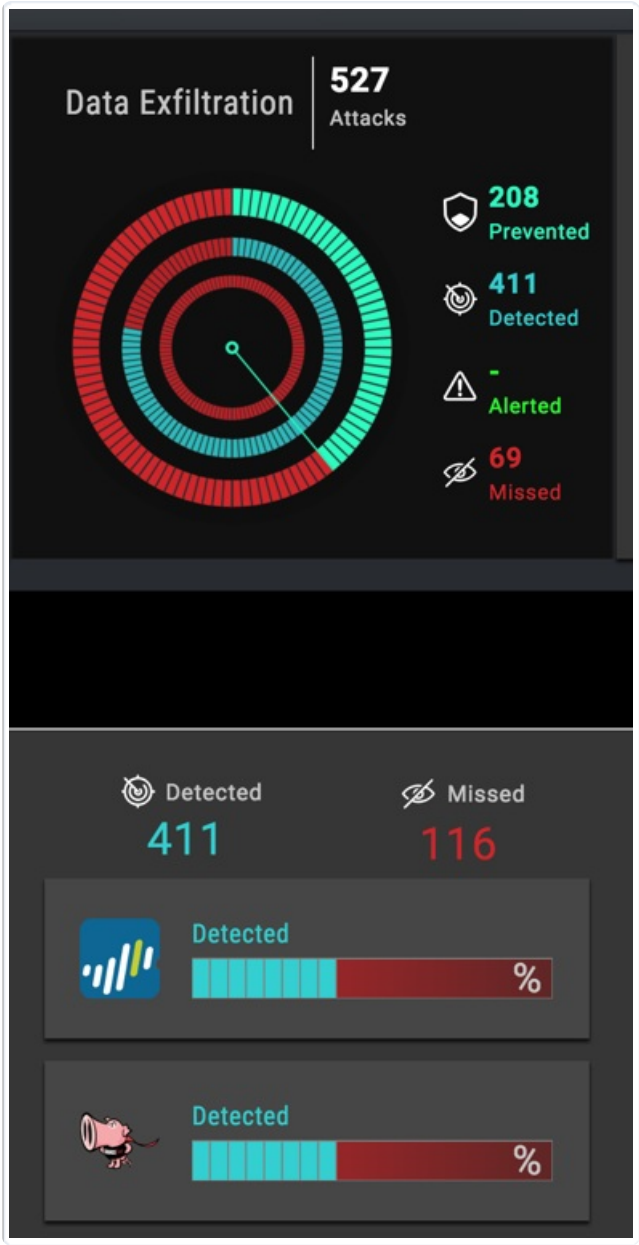
The Gauges page can be exported as a PDF. The is PDF is in Portrait mode with a white background and include the Gauges and Gauge details that are displaying at the time that **Save as PDF** is selected. To include details for all Gauges, click **Expand All Details** before exporting.

The Gauge graphics are all displayed at the top of the page. The Gauge Details panes for each of those graphics is listed on its own page. The panes include the four categories and graphics with the percentage for each of the security technologies.

In addition to exporting the entire Gauge page, you can export the Gauges and Gauge details as separate graphics to be integrated into external reports. The graphics are exported as PNG files and have transparent backgrounds.

Gauge use case examples

Consider the information you see in this Data Exfiltration Gauge and Details.



Data Exfil Gauge and Details

When you look at the Gauge, you can see that no Alerts occurred for any of the Actions. When you dig a little deeper by going into the Gauge details, you see that there are logs for a high percentage of the Actions. This demonstrates a good opportunity for policy tuning and reviewing existing content in your SIEM. It may also identify potential content that could be developed.

The technologies may identify the same Actions or they may each identify unique Actions. The bar charts add up to the total percentage.

Consider the Gauge Details for the Malicious File Transfer Gauge.

Expanding the details allows you to see the number of Jobs, Actions included in those Jobs, and number of Events that were generated. This helps you identify potential tuning opportunities with your Integrations and in the platform. Clicking

Analyze initiates the tuning process and workflow.

Malicious File Transfer Gauge and Details

In the Gauge Details, you see that there are Job Actions that were Prevented and Detected by unknown Security Technologies. Some of the possible reasons Actions fall into this category include:

- The Security Technology field mapping in the Validation Platform may need to be added or adjusted so the platform can recognize technology from the Integration.
- The Query or Advanced options of the Integration in the Validation Platform may need to be adjusted.
- Field Mappings in your SIEM or log manager may need to be tuned.
- Incorrect data is being delivered to the SIEM or is being parsed incorrectly.
- Data may not be sent (IP addresses stripped).
- Other parsing or data-related issues.
- Time synchronization may be off from reference time.