Reports overview

Create custom reports
Customized reports and dashboards enable you to pool the most meaningful data and insights about your organization's security posture into a more focused view based on what your organization or specific teams and stakeholders need to know and care about most. Customizing reports can increase the actionability of information and improve efficiencies across teams, because it reduces the workload of busy security teams and allows them to focus on the most critical vulnerabilities.

Before building custom views using tools such as PowerBI and Excel, you can enrich the native datasets provided by Microsoft's threat and vulnerability management solution with additional data from Microsoft Defender for Endpoint or a third-party tool of your choice.

Other benefits:

- **Report on key information and trends to top management and track business KPIs**. The reports will contain meaningful insights into the overall status of the vulnerability management program in your organization.
- **Use the data to create tasks or daily work items**. Only show actionable information your team needs.
- **Combine data from threat and vulnerability management with advanced filtering capabilities**. View insights from the vulnerability report and other information such as missing security updates, installed software, end-of-support products, and operating systems.
- **Optimize and streamline the end user experience according to your organization's needs**.

Let's look at some examples of reports that you will see in these templates:

Vulnerabilities report:

- Learn about the security posture of your organizations.
- Identify the most critical and exploitable vulnerabilities.
- View the most exposed devices distributed by operating systems.
- Drill down to investigate specific CVEs.

You can filter the report by the first time the CVE was detected in your org (e.g. show me only CVEs detected in the last 3 months), or by advanced properties such as Device tags, Device groups, and Device health (active\inactive).

Missing Windows security updates

- View all missing Windows security updates in your organization.
- Identify the most exposed operating systems.
- Search for one security update to get all the affected devices in one click.

You can filter the report by the associated CVEs criticality, by the age of each security update, or by advanced properties such as Device tags, Device groups, and Device health (active\inactive).

Software inventory

- Look at organizational software inventory.
- Explore the recent installations in your org including the devices involved, when, and what version.

You can filter the report by the number of the weaknesses associated with each software, by software name\vendor, or by advanced properties such as Device tags, Device groups, and Device health (active\inactive).

In addition to the three reports mentioned, find more report templates that you can customize including:

- End-of-support operating systems
- End-of-support software and versions
- Misconfigurations per device
- Software vulnerability recommendations and non-windows security updates
- Exposure score visualizations
- And more!

More resources:

Build OData queries with Microsoft Defender for Endpoint

Create custom reports using Microsoft Defender ATP APIs and Power BI

APIs you'll need to use

To use the entire template, you should use 7 different APIs:

Secure configuration assessment by machine

Software inventory assessment by machine

Software vulnerabilities assessment by machine

Machines

Exposure score / By machine groups

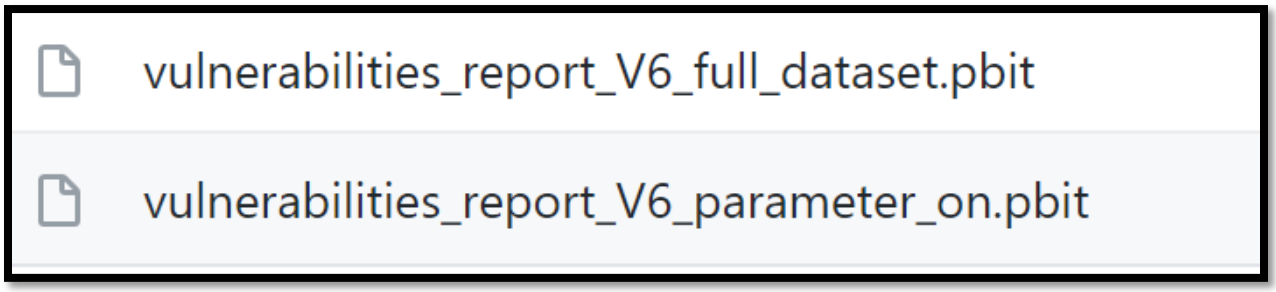
Get all recommendations

Get all vulnerabilities

Getting started

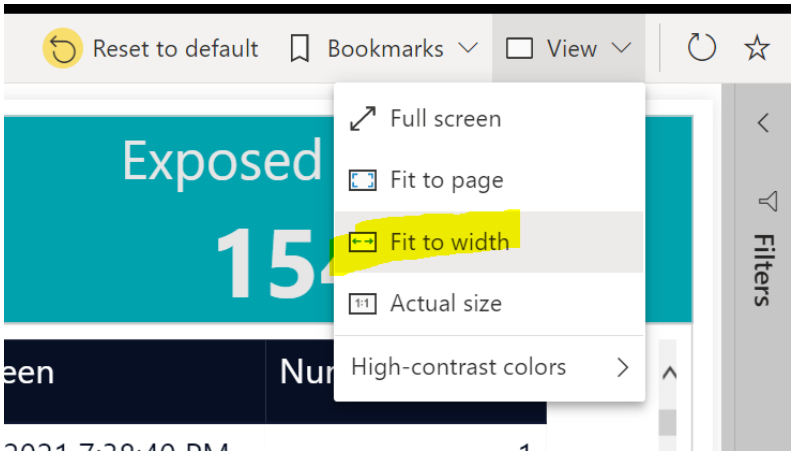
1. Download **Power BI for Desktop** and make sure you have the latest version installed. You can read some guidance if you are not familiar with Power BI. View general guidance about Microsoft Defender for Endpoint APIs and Power BI

2. Download the Power BI templates from GitHub



   a) **Small** organizations should download the file ends with "full_dataset"
   b) **Medium** or **large** organizations may not be able to use these templates due to PowerBI limitations, but can try download the file ends with "parameter_on".

3. Open Power BI for Desktop and load the template you download. Connect all the 7 APIs (OData source) with your MDE credentials.
4. It is recommended to understand the relationships model in this template in order to do your own improvements.
5. Take a look at the report, make changes or adjustments based on your org's needs and metrics.
6. After completing the report edits, **Save** it and click on **Publish**. Choose the workspace you want this report to be presented. Once it is published in the Web, you can work with the report and no longer need the Power BI for Desktop.
7. In the Web app report, it is recommended to change the **View** settings to "**Fit to width**":



How to handle with a large amount of data?

In case the data loading takes a lot of time (hours), you can use the parameter we created and is built-in in the template. Using the parameters means that only a **subset** of the data in the Desktop app will be shown, and will help with the loading time.

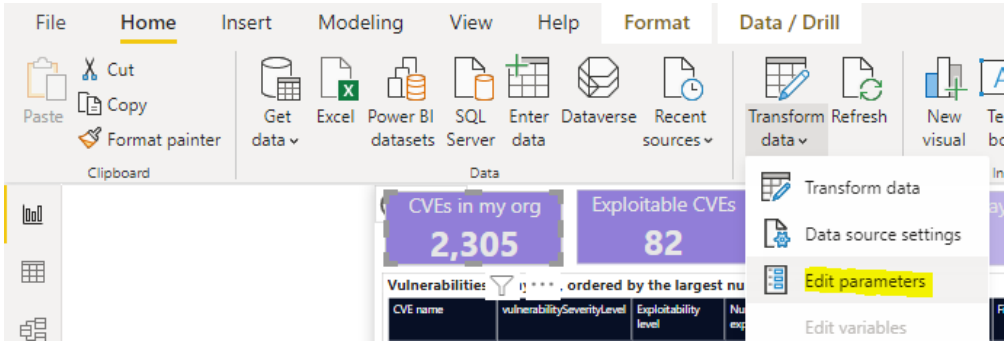
No worries, once publishing the final version to the Web report, you can turn-off the parameter to get all the data.

The parameter filters the heaviest APIs (5 out of the 7: Secure configuration assessment by machine, Software inventory assessment by machine, Software vulnerabilities assessment by machine, Machines, Get all vulnerabilities) in order to limit the results. It will bring a subset of the data, up to 10K-50K records, instead all of them.

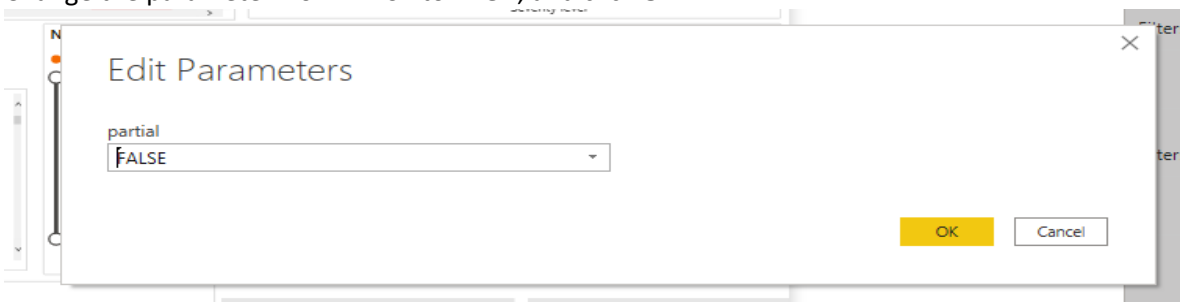
Please follow these instructions to use the parameter:

1. Log in to Power BI Desktop and load the template you downloaded

2. In the menu, go to **Home** -> **Transform data** -> **Edit parameters**



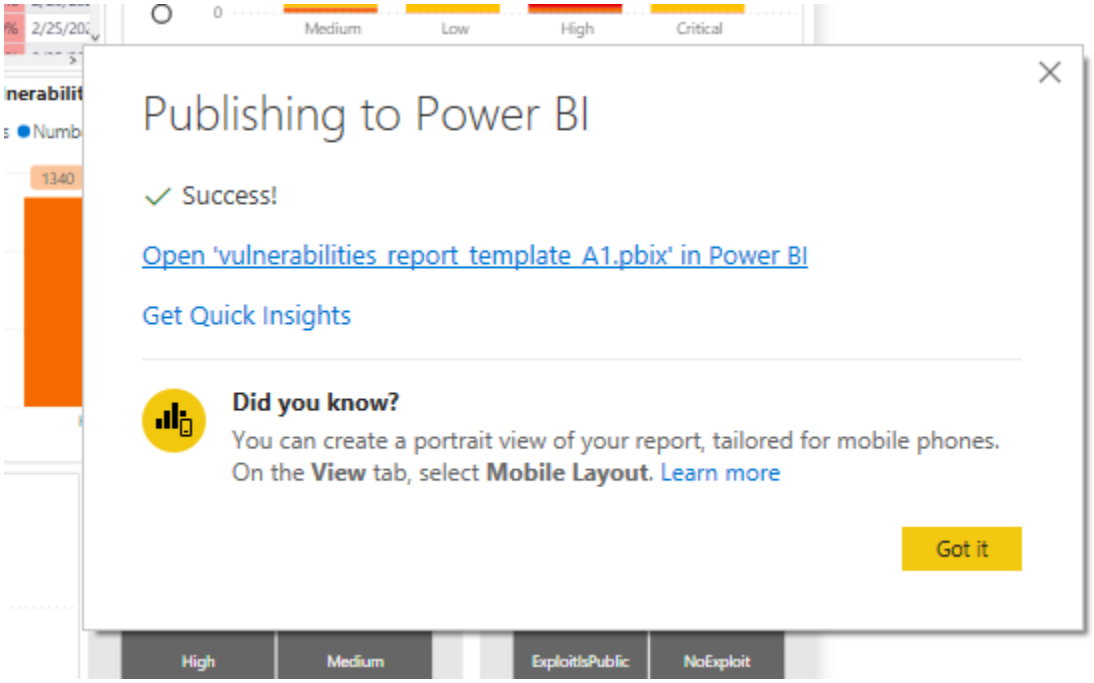
3. Change the parameter from FALSE to ***TRUE***, and click **OK**



4. Click on "**Apply changes**" in the yellow message bar

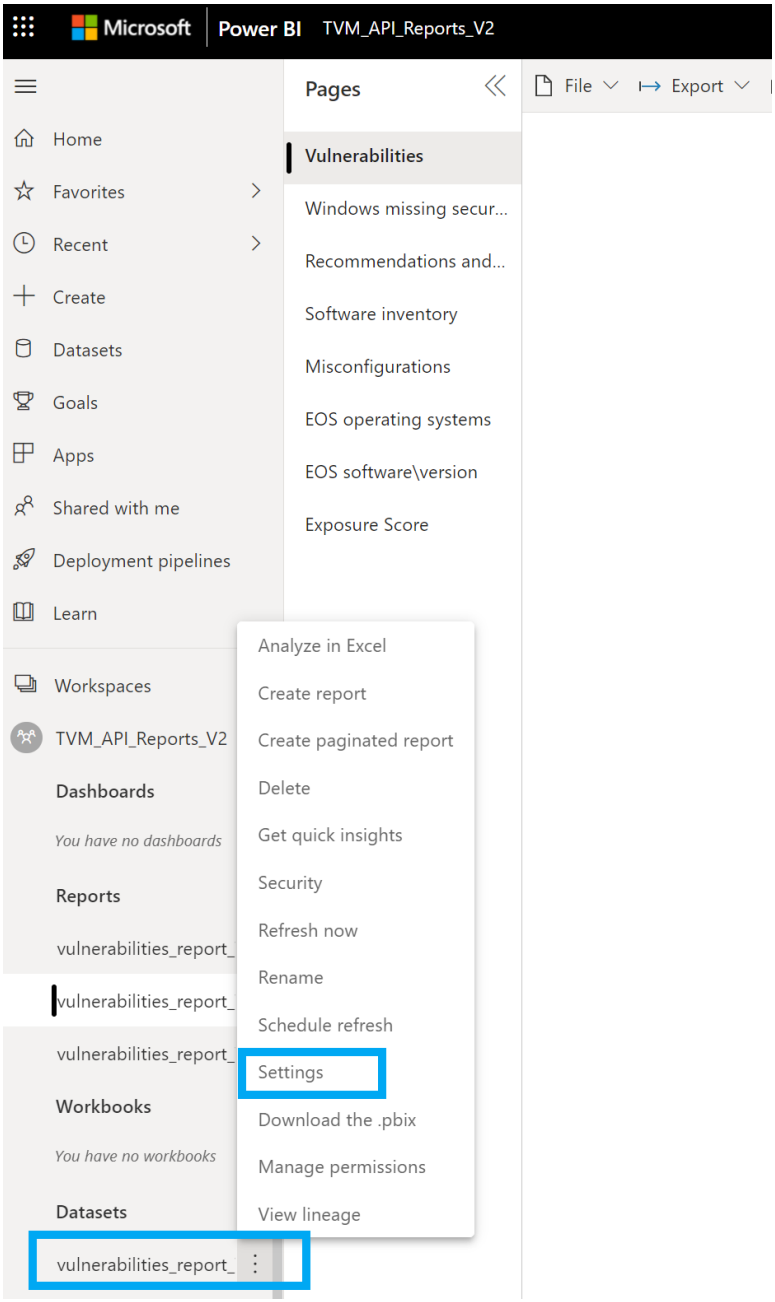
5. Now 5 out of the 7 APIs will be updated. Wait a few minutes until it's done.

6. **Save** and **Publish** the report in the relevant workspace. Once published, go to the workspace in the Web (you can **click on the link** you got after publishing ("open XXXXXX…. In Power BI") –

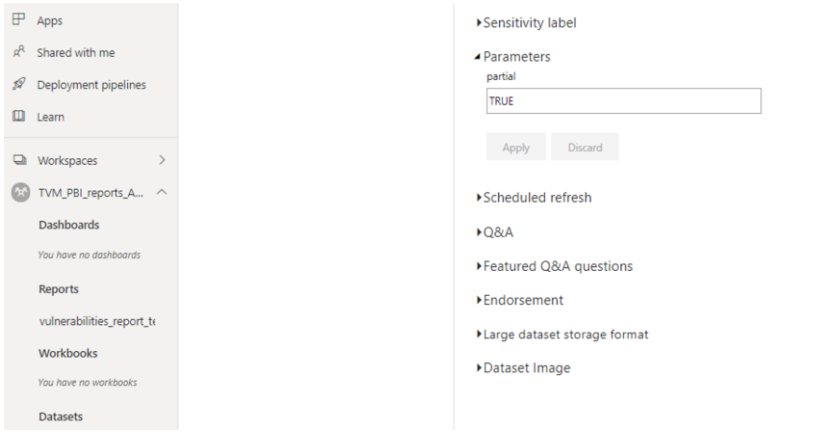


7. After clicking on the link, now you have report open with the partial data

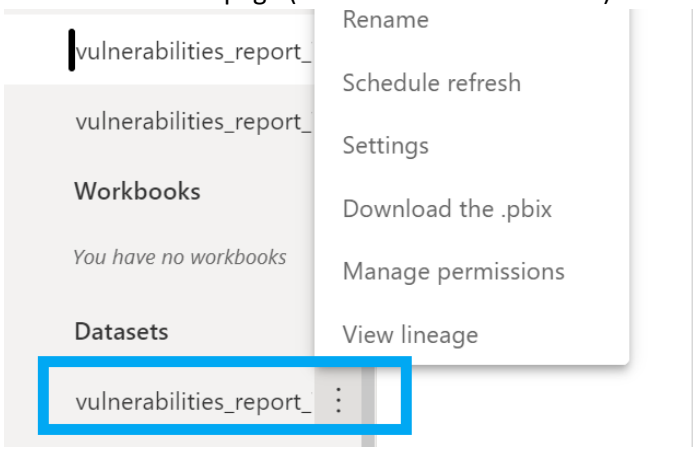
8. In the Web app, go to the **Dataset settings**:


Microsoft
Power BI
TVM_API_Reports_V2
Home
Favorites
Recent
Create
Datasets
Goals
Apps
Shared with me
Deployment pipelines
Learn
Workspaces
TVM_API_Reports_V2
Dashboards
You have no dashboards
Reports
vulnerabilities_report_
vulnerabilities_report_
vulnerabilities_report_
Workbooks
You have no workbooks
Datasets
vulnerabilities_report_
Pages
Vulnerabilities
Windows missing secur...
Recommendations and...
Software inventory
Misconfigurations
EOS operating systems
EOS software\version
Exposure Score
File
Export
Analyze in Excel
Create report
Create paginated report
Delete
Get quick insights
Security
Refresh now
Rename
Schedule refresh
Settings
Download the .pbix
Manage permissions
View lineage

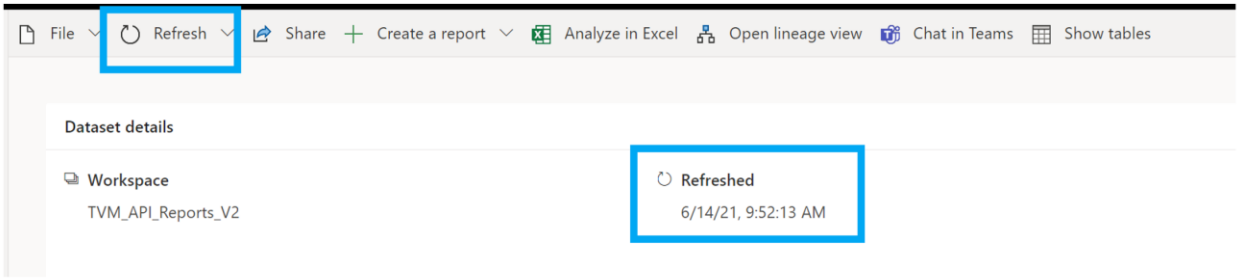
9. Go to **Parameters** section, change the value to ***FALSE*** and click **Apply**:



10. Go to the **Dataset** page (click on the dataset name):

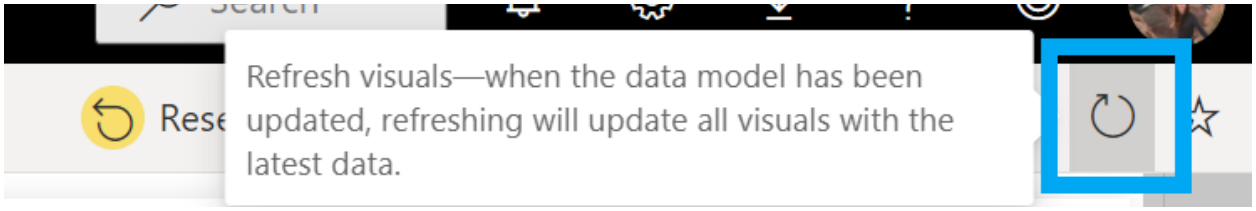


11. **Refresh** dataset. Wait until you see the “Refreshed” timestamp up-to-date, it is going to take a few minutes or longer.



12. Go back to the report

13. **Refresh** the visuals



14. Wait a few seconds, and you are done! Now you have the report with the full data from threat & vulnerability management.