Detections

https://campus.barracuda.com/doc/98225566/

The Detections page shows files found that have sensitive data or are malicious.

Data Inspector continually scans your system for new files. You will receive an alert on the page as new issues are found.

Three tabs on this page show the status of each file.

- **Unresolved** – Files identified by Barracuda Data Inspector as malicious or containing sensitive data that have not yet been remediated.
- **In Progress** – Remediation actions have been taken on the files shown here. (See **Remediate** below to learn more.) This is a temporarily location. As the action on each file completes, it is moved to the **Resolved** tab.
- **Resolved** – Files that have been remediated. The **Action** column shows the remediation action performed.

  Files that are *Unshared* are scanned again. Because the initial issue (sensitive data, malicious payload) is likely still present, these files will return to the **Unresolved** tab.

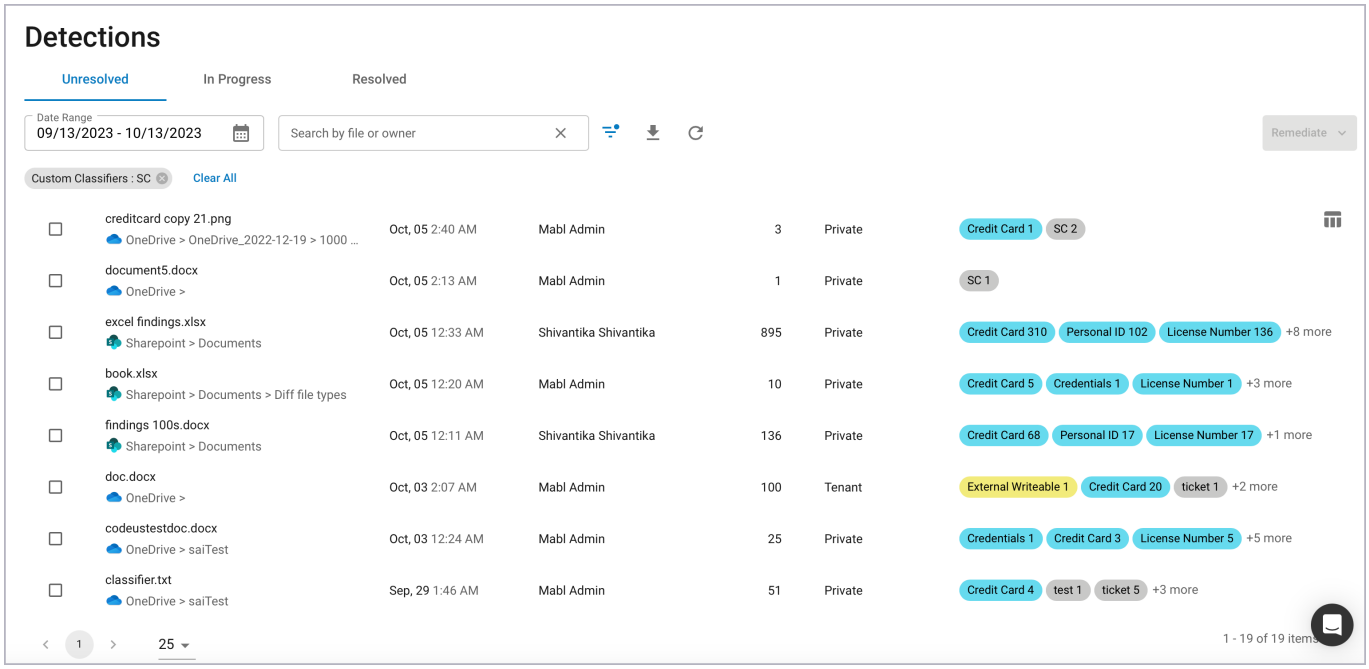


Table columns are:

- **File** – A file flagged by Barracuda Data Inspector as malicious or containing sensitive content.
- **Platform** – The infrastructure holding the file. This will be either Microsoft OneDrive or Sharepoint.
- **Last Detected** – After files are edited or changed in some way, they will be rescanned. Last

Detected denotes the most recent time a file was found to be malicious or have sensitive content.

- **Owner** – the owner of the file.
- **Violations** – The total number of malicious or sensitive content incidences in the file.
- **Sharing** – Access granted to a file.
  - **Private** – Only accessible to the owner.
  - **Internal** – Shared with others within the organization.
  - **External** – Shared outside the organization. (Can also include sharing within the organization.)
  - **Public** – There are no restrictions to file access. Open to anyone.
- **Classifiers** – Categories of sensitive data that describe the file.
  - Supported categories include credentials, credit card, license number, malicious content, passport, personal ID, personal medical ID, suspicious content, and tax ID.
  - The color of the classification label indicates the type of information detected.
    - **Blue labels** – Indicate the file contains sensitive information such as a license number or tax ID.
    - **Yellow labels** – Indicate sharing violations.
    - **Red labels** – Indicate that the file is malicious.
    - **Gray labels** – Indicate the file contains information from keyword or regex (regular expression) classifiers that have been set on the Classifiers page.
  - The number inside the classification label denotes the number of times the sensitive information was detected in the file.
- **Action** – This column is found on the **In Progress** and **Resolved** tabs and shows the remediation action taken.

Filtering Page Results

There are multiple tools to help limit the files displayed to only those you are interested in.

Sort by Column

Click the top of the **File**, **Last Detected**, or **Violations** columns to sort. **File** will sort by file names alphabetically. **Last Detected** is the default and sorts most recent to least recent. **Violations** sorts the table from the files with the fewest to the most violations. Clicking a second time on any of these will reverse the order (i.e. least recent to most recent).

Search Box

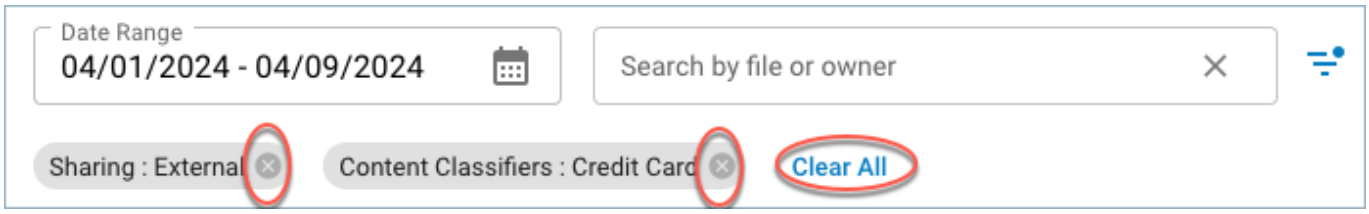
Add text to the search field to find a file name, file owner, or file creator match.

Filter Button

Click the filter button to open a list to narrow down search results. Select from *Platform*, *Sharing*,

and *Classifier* options. (See above for descriptions of each.) Options with zero instances or those not compatible with options already checked are grayed out and cannot be selected.

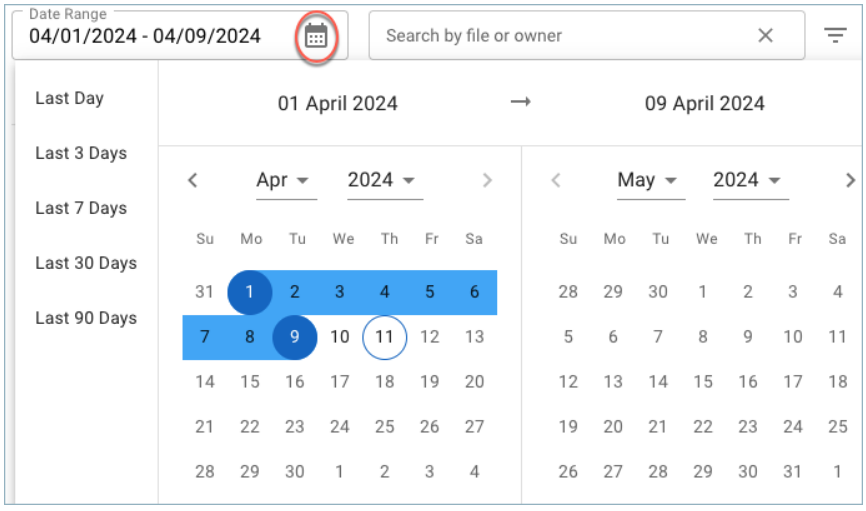
Once a box is checked, a corresponding filter chip will appear under the search box. Filters can be removed by clicking the **X** next to one or clicking the **Clear All** link.



Date Range

Limit page results to those that occurred in a given time period.

Click the calendar icon on the **Date Range** field to open the date range selector. Click on one of the built in presets at left (i.e. *Last 3 Days*, *Last 30 Days*, etc.) or select a range by clicking on the days in the calendar.



View File Details

Click on one of the table rows to see the details of that file.

Other Detections Page Options

Click the reload icon to view the latest file detections. Note: any implemented text search, selected filters, or date ranges will be retained. To restore detection results to default, reload the browser window.

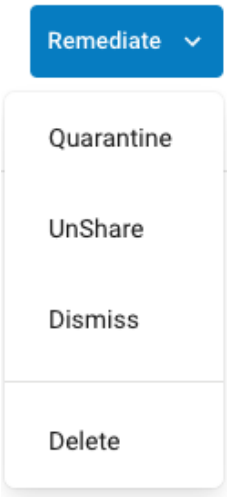
The button will export up to 10,000 activities and will be limited by any active searches, filters or date ranges.

Click the Select Columns icon at far right to limit the columns displayed. *Last Detected, Owner/Creator*, *Violations*, *Sharing*, and *Classifiers* can be added or removed. *File* is always displayed and cannot be deselected.

Click the back **<** or forward **>** arrows or one of the numbers at the bottom to view another page of file detections. The number of files shown per page can be changed via the dropdown menu 25.

Remediate Files

Click the **Remediate** button to manage files found to be malicious or have sensitive data. There are four options:



- **Quarantine** – Moves the file to a Quarantine directory with limited access. Within the Detections page it transfers from the **Unresolved** tab to the **In Progress** tab. Once the action is complete, it transfers again from **In Progress** to **Resolved**.
- **UnShare** – Changes the file access permissions to Private and transfers it from the **Unresolved** tab to **In Progress** and finally to **Resolved** once the action is complete. At that point only the file owner will have access to it. Once this is done, Barracuda Data Inspector will rescan the file.

If it is malicious or still contains sensitive data, it will again be added to Detections as **Unresolved**.

- **Dismiss** – Transfers the file to the **Resolved** tab without changing anything else. This would generally be used when the file is determined to be ok as it is.
- **Delete** – Moves files to the user's Recycle Bin. Files in the Recycle Bin will not be scanned, but can be recovered if needed.

Figures