Forensics

Data Infrastructure Insights

NetApp
October 29, 2024

Table of Contents

Forensics

Forensics - All Activity

The All Activity page helps you understand the actions performed on entities in the Workload Security environment.

Examining All Activity Data

Click **Forensics > Activity Forensics** and click the **All Activity** tab to access the All Activity page.
This page provides an overview of activities in your environment, highlighting the following information:

- A graph showing *Activity History* (accessed per minute/per 5 minutes/per 10 minutes based on selected global time range)

  You can zoom the graph by dragging out a rectangle in the graph. The entire page will be loaded to display the zoomed time range. When zoomed in, a button is displayed that lets the user zoom out.

- A chart of *Activity Types*. To obtain activity history data by activity type, click on corresponding x-axis label link.
- A chart of Activity on *Entity Types*. To obtain activity history data by entity type, click on corresponding x-axis label link.
- A list of the *All Activity* data

The **All Activity** table shows the following information. Note that not all of these columns are displayed by default. You can select columns to display by clicking on the "gear" icon.

- The **time** an entity was accessed including the year, month, day, and time of the last access.
- The **user** that accessed the entity with a link to the User information.

- The **activity** the user performed. Supported types are:
  - **Change Group Ownership** - Group Ownership is of file or folder is changed. For more details about group ownership please see this link.
  - **Change Owner** - Ownership of file or folder is changed to another user.
  - **Change Permission** - File or folder permission is changed.
  - **Create** - Create file or folder.
  - **Delete** - Delete file or folder. If a folder is deleted, *delete* events are obtained for all the files in that folder and subfolders.
  - **Read** - File is read.
  - **Read Metadata** - Only on enabling folder monitoring option. Will be generated on opening a folder on Windows or Running “ls” inside a folder in Linux.
  - **Rename** - Rename file or folder.
  - **Write** - Data is written to a file.
  - **Write Metadata** - File metadata is written, for example, permission changed.
  - **Other Change** - Any other event which are not described above. All unmapped events are mapped to “Other Change” activity type. Applicable to files and folders.

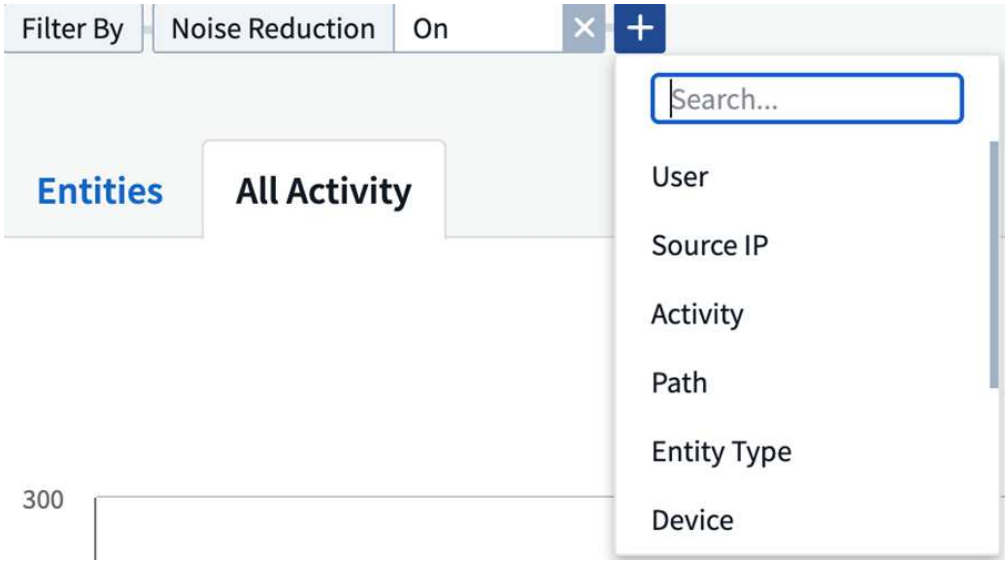
- The **Path** to the entity with a link to the Entity Detail Data
- The **Entity Type**, including entity (i.e. file) extension (.doc, .docx, .tmp, etc.)
- The **Device** where the entities reside
- The **Protocol** used to fetch events.
- The **Original Path** used for rename events when the original file was renamed. This column is not visible in the table by default. Use the column selector to add this column to the table.
- The **Volume** where the entities reside. This column is not visible in the table by default. Use the column selector to add this column to the table.

Filtering Forensic Activity History Data

There are two methods you can use to filter data.

1. Hover over the field in the table and click the filter icon that appears. The value is added to the appropriate filters in the top *Filter By* list.
2. Filter data by typing in the *Filter By* field:

   Select the appropriate filter from the top 'Filter By' widget by clicking the **[+]** button:



   Enter the search text

   Press Enter or click outside of the filter box to apply the filter.

You can filter Forensic Activity data by the following fields:

- The **Activity** type.
- **Source IP** from which the entity was accessed. You must provide a valid source IP address in double quotes, for example "10.1.1.1.". Incomplete IPs such as "10.1.1.**", "10.1.**.*", etc. will not work.
- **Protocol** to fetch protocol-specific activities.
- **Username** of the user performing the activity. You need to provide the exact Username to filter. Search with partial username, or partial username prefixed or suffixed with '*' will not work.
- **Noise Reduction** to filter files which are created in the last 2 hours by the user. It is also used to filter

temporary files (for example, .tmp files) accessed by the user.

- **Domain** of the user performing the activity. You need to provide the **exact domain** to filter. Searching for partial domain, or partial domain prefixed or suffixed with wildcard ('*'), will not work. *None* can be specified to search for missing domain.

The following fields are subject to special filtering rules:

- **Entity Type**, using entity (file) extension - it is preferable to specify exact entity type within quotes. For example *“txt”*.
- **Path** of the entity - Directory Path filters (path string ending with /) up to 4 directories deep are recommended for faster results. For example, */home/userX/nested1/nested2/* OR *"/home/userX/nested1/nested2/"*. See the table below for more details.
- **User** performing the activity - it is preferable to specify the exact user within quotes. For example, *"Administrator"*.
- **Device** (SVM) where entities reside
- **Volume** where entities reside
- The **Original Path** used for rename events when the original file was renamed.

The preceding fields are subject to the following when filtering:

- Exact value should be within quotes: Example: "searchtext"
- Wildcard strings must contain no quotes: Example: searchtext, *searchtext*, will filter for any strings containing ‘searchtext’.
- String with a prefix, Example: searchtext* , will search any strings which start with ‘searchtext’.

Activity Forensics Filter Examples:

User applied Filter expression	Expected Outcome	Performance assessment	Comment
Path = /home/userX/nested1/nested2/ or /home/userX/nested1/nested2/* or "/home/userX/nested1/nested2/"	Recursive lookup of all files and folders under given directory	Fast	Directory searches up to 4 directories will be fast.
Path = /home/userX/nested1/ or /home/userX/nested1/* or "/home/userX/nested1/"	Recursive lookup of all files and folders under given directory	Fast	Directory searches up to 4 directories will be fast.
Path = /home/userX/nested1/test* or /home/userX/nested1/test	Recursive lookup of all files and folders under given path regex(test* could mean file OR directory OR Both)	Slower	Directory+File regex search will be slower to search on compared to Directory searches.

User applied Filter expression	Expected Outcome	Performance assessment	Comment
Path = /home/userX/nested1/nested2/nested3/ or /home/userX/nested1/nested2/nested3/* or "/home/userX/nested1/nested2/nested3/"	Recursive lookup of all files and folders under given directory	Slower	More than 4 directories searches are slower to search on.
Path=*userX/nested1/test*	Recursive lookup of all files and folders under given wildcard path string(test* could mean file OR directory OR Both)	Slowest	Leading wildcard search are slowest searches.
Any other Non path based filters. User and Entity Type filters recommended to be in quotes e.g., User="Administrator" Entity Type="txt"		Fast	

NOTE:

1. The Activity count displayed alongside the All Activity icon is rounded off to 30 mins when the selected time range spans more than 3 days. e.g., a time range of *Sept 1st 10:15 am to Sept 7th 10:15 am* will show Activity counts from Sept 1st 10:00 am to Sept 7th 10:30 am.
2. Likewise the count metrics shown in Activity Types, Activity on Entity Types, and Activity History graph are rounded off to 30 mins when the selected time range spans more than 3 days.

Sorting Forensic Activity History Data

You can sort activity history data by *Time, User, Source IP, Activity,* and *Entity Type*. By default, the table is sorted by descending *Time* order, meaning the latest data will be displayed first. Sorting is disabled for *Device* and *Protocol* fields.

User Guide for Asynchronous Exports

Overview

The Asynchronous Exports feature in Storage Workload Security is designed to handle large data exports.

Step-by-Step Guide: Exporting Data with Asynchronous Exports

1. **Initiate Export**: Select the desired time duration and filters for the export and click on the export button.
2. **Wait for Export to Complete**: The processing time can range from a few minutes to a few hours. You may need to refresh the forensics page a few times. Once the export job is complete, the "Download last export CSV file" button will be enabled.
3. **Download**: Click on the "Download last created export file" button to get the exported data in a .zip format. This data will be available for download until the user initiates another Asynchronous Export or 3 days have elapsed, whichever occurs first. The button will remain enabled until another Asynchronous Export is

initiated.

4. **Limitations**:
    - The number of asynchronous downloads is currently limited to 1 per user and 3 per tenant.
    - The exported data is limited to a maximum of 1 million records.

A sample script to extract forensic data via API is present at */opt/netapp/cloudsecure/agent/export-script/* on the agent. See the readme at this location for more details about the script.

Column Selection for All Activity

The *All activity* table shows select columns by default. To add, remove, or change the columns, click the gear icon on the right of the table and select from the list of available columns.

Activity History Retention

Activity history is retained for 13 months for active Workload Security environments.

Applicability of Filters in Forensics Page

Filter	What it does	Example	Applicable for these Filters	Not applicable for these filters	Result
* (Asterisk)	enables you to search for everything	Auto*03172022 If search text contains hyphen or underscore, give expression in brackets. e.g., (svm*) for searching svm-123	User, PATH, Entity Type, Device, Volume, Original Path		returns all resources that start with “Auto" and end with “03172022”
? (question mark)	enables you to search for a specific number of characters	AutoSabotageUser1_03172022?	User, Entity Type, Device, Volume		returns AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022B, AutoSabotageUser1_031720225, and so on
OR	enables you to specify multiple entities	AutoSabotageUser1_03172022 OR AutoRansomUser4_03162022	User, Domain, PATH, Entity Type, Original Path		returns any of AutoSabotageUser1_03172022 OR AutoRansomUser4_03162022

Filter	What it does	Example	Applicable for these Filters	Not applicable for these filters	Result
NOT	allows you to exclude text from the search results	NOT AutoRansomUser4_03162022	User,Domain, PATH, Entity Type, Original PATH	Device	returns everything that does not start with"AutoRansomUser4_03162022”
None	searches for NULL values in all fields	None	Domain		returns results where the target field is empty

Path / Original path Search

Search results with and without / will be different

/AutoDir1/AutoFile	Works
AutoDir1/AutoFile	Doesn’t work
/AutoDir1/AutoFile (Dir1)	Dir1 Partial substring doesn’t work
"/AutoDir1/AutoFile03242022"	Exact search works
Auto*03242022	Doesn’t work
AutoSabotageUser1_03172022?	Doesn’t work
/AutoDir1/AutoFile03242022 OR /AutoDir1/AutoFile03242022	Works
NOT /AutoDir1/AutoFile03242022	Works
NOT /AutoDir1	Works
NOT /AutoFile03242022	Doesn’t work
*	Shows all the entries

Local root SVM user activity changes

If a local root SVM user is performing any activity, the IP of the client on which the NFS share is mounted is now considered in the username, which will be shown as root@<ip-address-of-the-client> in both forensic activity and user activity pages.

For example:

- If SVM-1 is monitored by Workload Security, and the root user of that SVM mounts the share on a client with IP address 10.197.12.40, the username shown in forensic activity page will be *root@10.197.12.40*.
- If the same SVM-1 is mounted into another client with IP address 10.197.12.41, the username shown in forensic activity page will be *root@10.197.12.41*.

*• This is done to segregate NFS root user activity by IP address. Previously, all the activity was considered to be done by *root* user only, with no IP distinction.

Troubleshooting

Problem	Try This
In the “All Activities” table, under the ‘User’ column, the user name is shown as: “ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817” or "ldap:default:80038003”	Possible reasons could be: 1. No User Directory Collectors have been configured yet. To add one, go to **Workload Security > Collectors > User Directory Collectors** and click on **+User Directory Collector**. Choose *Active Directory* or *LDAP Directory Server*. 2. A User Directory Collector has been configured, however it has stopped or is in error state. Please go to **Collectors > User Directory Collectors** and check the status. Refer to the User Directory Collector troubleshooting section of the documentation for troubleshooting tips. After configuring properly, the name will get automatically resolved within 24 hours. If it still does not get resolved, check if you have added the correct User Data Collector. Make sure that the user is indeed part of the added Active Directory/LDAP Directory Server.
Some NFS events are not seen in UI.	Check the following: 1. A user directory collector for AD server with POSIX attributes set should be running with the unixid attribute enabled from UI. 2. Any user doing NFS access should be seen when searched in the user page from UI 3. Raw events (Events for whom the user is not yet discovered) are not supported for NFS 4. Anonymous access to the NFS export will not be monitored. 5. Make sure NFS version used in lesser than NFS4.1.
After typing some letters containing a wildcard character like asterisk (*) in the filters on the Forensics *All Activity* or *Entities* pages, the pages load very slowly.	An asterisk (*) in the search string searches for everything. However, leading wildcard strings like *<searchTerm> or *<searchTerm>* will result in a slow query. To get better performance, use prefix strings instead, in the format <searchTerm>* (in other words, append the asterisk (*) *after* a search term). Example: use the string *testvolume**, rather than **testvolume* or **test*volume*. Use a directory search to see all activities underneath a given folder recursively (Hierarchical search). e.g., /path1/path2/path3/ or “/path1/path2/path3/” will list all the activities recursively under /path1/path2/path3. Alternatively use the "Add To Filter" option under the All Activity tab.”
I am encountering a "Request failed with status code 500/503" error when using a Path filter.	Try using a smaller date range for filtering records.

Forensic UI is loading data slowly when using the *path* filter.	Directory Path filters (path string ending with /) up to 4 directories deep are recommended for faster results. e.g., If the directory path is /Aaa/Bbb/Ccc/Ddd, try searching for /Aaa/Bbb/Ccc/Ddd/ or "/Aaa/Bbb/Ccc/Ddd/" to load data faster.

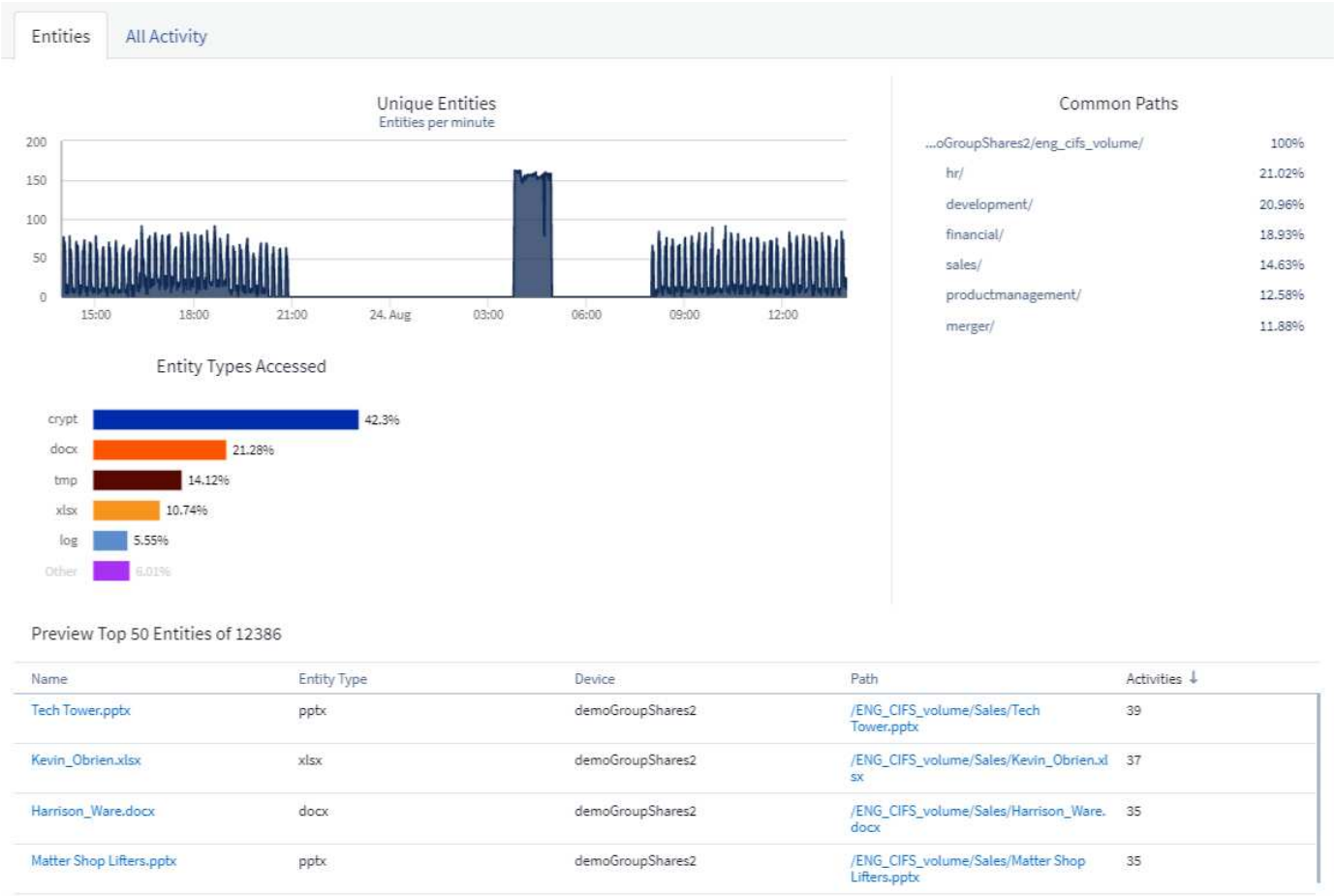
Forensic Entities Page

The Forensics Entities page provides detailed information about entity activity in your environment.

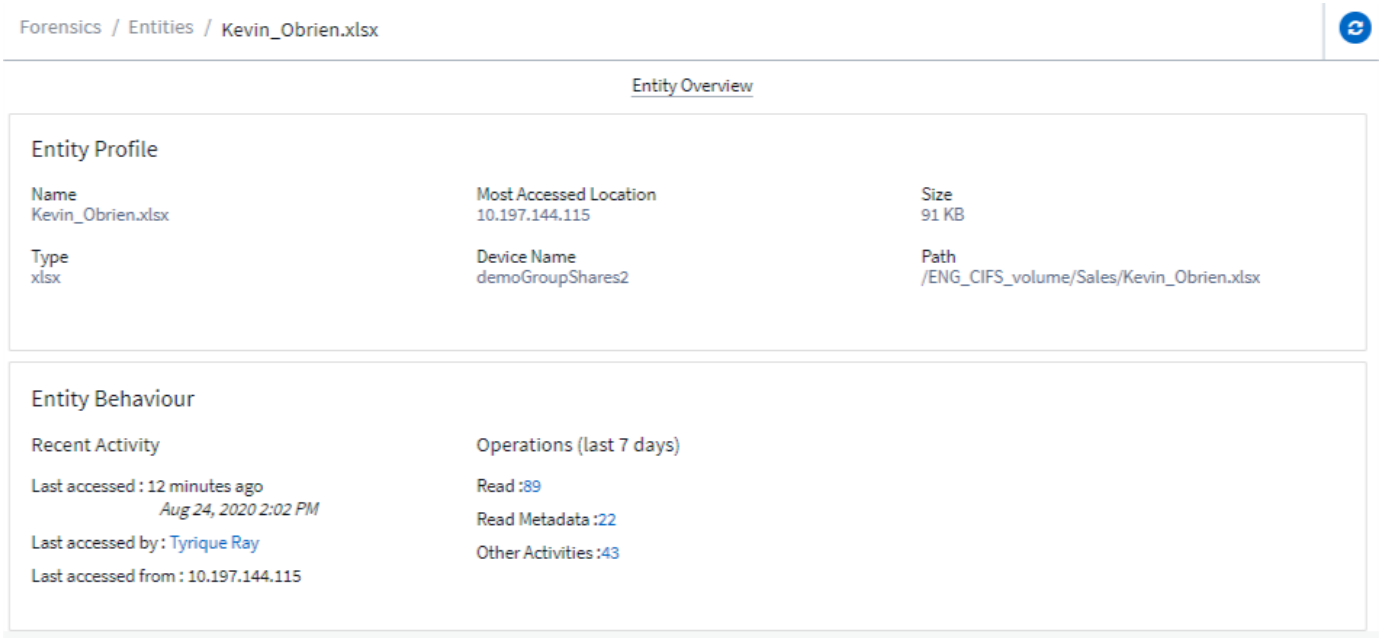
Examining Entity Information

Click **Forensics > Activity Forensics** and click the *Entities* tab to access the Entities page.

This page provides an overview of entity activity in your environment, highlighting the following information:
* A graph showing *Unique Entities* accessed per minute
* A chart of *Entity Types Accessed*
* A breakdown of the *Common Paths*
* A list of the *Top 50 Entities* out of the total number of entities



Clicking on an entity in the list opens an overview page for the entity, showing a profile of the entity with details like name, type, device name, most accessed location IP, and path, as well as the entity behavior such as the user, IP, and time the entity was last accessed.



Forensic User Overview

Information for each user is provided in the User Overview. Use these views to understand user characteristics, associated entities, and recent activities.

User Profile

User Profile information includes contact information and location of the user. The profile provides the following information:

- Name of the user
- Email address of the user
- User's Manager
- Phone contact for the user
- Location of the user

User Behavior

The user behavior information identifies recent activities and operations performed by the user. This information includes:

- Recent activity
  - Last access location
  - Activity graph
  - Alerts
- Operations for the last seven days
  - Number of operations

Refresh Interval

The User list is refreshed every 12 hours.

Retention Policy

If not refreshed again, the User list is retained for 13 months. After 13 months, the data will be deleted.
If your Workload Security environment is deleted, all data associated with the environment is deleted.