

# Endpoint Detection and Response (EDR)

EventTracker v9.x

## Abstract

This document gives a brief overview of what Endpoint Detection and Response (EDR) is, what are the uses of Endpoint Detection and Response and why you should use it in the EventTracker version 9.x.

EDR is an advanced technology of IT/network security to address the need for detection and prevention of attacks through endpoints in the network.

EventTracker EDR platform is an integrated security solution providing an additional layer of security and visibility for your enterprise across your IT network.

EventTracker's EDR capabilities mainly include:

- Endpoint data collection
- Detection of anomalies
- Alerts
- Data recording
- Response

## Audience

This guide is for all EventTracker users responsible for investigating and managing network security. This guide assumes that you have the knowledge of your entire enterprise networking.

EventTracker v9.x users who want to know about the Endpoint Detection and Response.

*The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.*

*This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.*

*Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.*

*Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.*

*The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.*

*© 2021 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

## Table of Contents

1.	Endpoint Detection and Response .....	4
2.	Uses of EDR.....	4
3.	EDR vs Anti-virus.....	4
4.	Introducing EDR in EventTracker v9.x .....	5
5.	Accessing the EDR from EventTracker .....	6
6.	Dashboard .....	8
6.1	Groups Pane.....	9
6.2	Overview of sensors in Groups Pane .....	11
6.3	Pending Analyst Review pane.....	13
6.4	Overview of the Pending Processes .....	20
6.5	Action Taken Processes Pane .....	23
6.6	Overview of the Action Taken Processes .....	25
7.	Processes page .....	25
7.1	Vendors.....	26
7.1.1	Observed Vendors.....	28
7.1.2	Collection.....	32
7.1.3	Approved Vendors.....	33
7.1.4	Approved Collection .....	34
7.1.5	Import Vendors .....	36
7.1.6	Export Vendors.....	36
7.2	Rules.....	37
7.3	Allowed Process.....	38
7.4	Denied Process .....	41
7.5	Research Process .....	43
8.	Sensors page.....	45
8.1	Edit Group Info.....	47
8.2	Edit Sensor Info.....	50
9.	Agent Resource Utilization .....	52

# 1. Endpoint Detection and Response

Endpoints serve as gateways to an enterprise network and create points of entry which can be used for malicious attack. Therefore, it is crucial to secure endpoints and this can be done efficiently using Endpoint security software like EventTracker EDR.

EDR tool is an adaptive, superior and thorough technology of protecting the endpoints in your network. Endpoint Detection and Response Solutions are exclusively designed for monitoring and responding to the Advanced Internet Threats.

The EDRs is installed as agents or sensors for the endpoints, from where security data are collected and sent to a centralized location for further analysis.

EDR solutions help in analyzing and identifying the patterns and detecting malware, which can be notified as alerts for remedial actions or any investigation.

## 2. Uses of EDR

To safeguard the network/ Endpoints in your network, you must use Endpoint Detection and Response tool as an advanced security solution.

You should install Endpoint Detection and Response for the following reasons:

- To check if the adversaries have already installed malware and moved laterally in the networks.
- To detect risky behavior on the network.
- To have complete visibility across the network and endpoints 24/7.
- To access any damages from the malware on the business.
- To check if the legacy devices are putting the network at risk.
- To protect the network from vulnerabilities before patching occurs.
- To reduce false positives using threat intelligence and to prioritize finite resources.
- To identify and investigate the advanced threat.

## 3. EDR vs Anti-virus

EDR solutions have many advantages which are not offered by traditional antivirus software. EDR provides next level of protection over antivirus.

An EDR security solution is centrally managed and remotely controlled security operations. EDR has a wider range of advanced features and automated tools to protect against different types of security attacks. It

covers your entire network. Antivirus provides just one aspect of endpoint protection platforms. Antivirus covers a single endpoint and only detects and blocks malicious files.

EDR	Antivirus
Protects complete networks and all their endpoints. Security solution for the entire organization.	Protects individual devices: Security solution for each workstation.
Threat identification and protection: Includes endpoint protection capabilities such as anti-malware, firewalls	Threat identification: Detects different types of malware including viruses.
Dashboards, reports and alert warnings to help continuous monitoring.	Alerts
Incident investigations and Response.	Scheduled scans
Identifies and blocks lateral movement across networks. It provides post-breach visibility.	

## 4. Introducing EDR in EventTracker v9.x

EventTracker v9.x has integrated EDR into its platform and these works together in strengthening your network security. EDR was introduced in EventTracker to solve post-breach visibility problems and prevention.

Over the period it was observed that the attackers were targeting the endpoints, which the traditional antivirus was not capable of detecting. So, to protect the endpoints in the network the Endpoint Detection and Response was introduced.

Endpoint Detection and Response services include the following:

- Application safe listing
- Forensic data gathering
- Host system visibility
- Threat intelligence sharing
- Low resource consumption
- Rich management console

## 5. Accessing the EDR from EventTracker

- Once you log into the EventTracker console with the username and password, **Home** page opens.

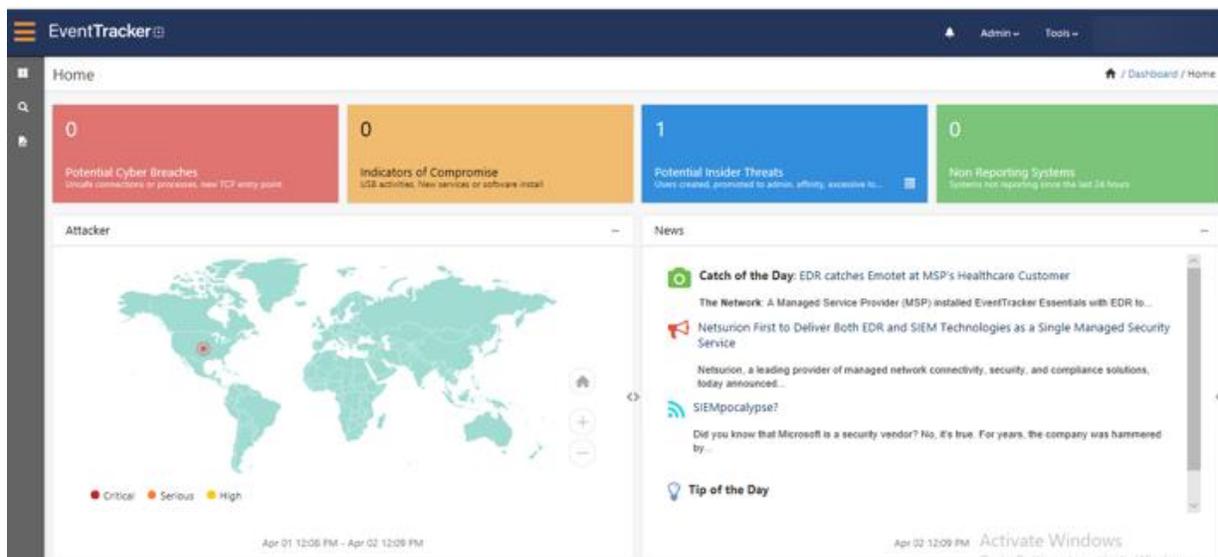


Figure 1

- On the left Ribbon, click the **Dashboard** icon in the upper left corner and select **EDR** from the dropdown menu.

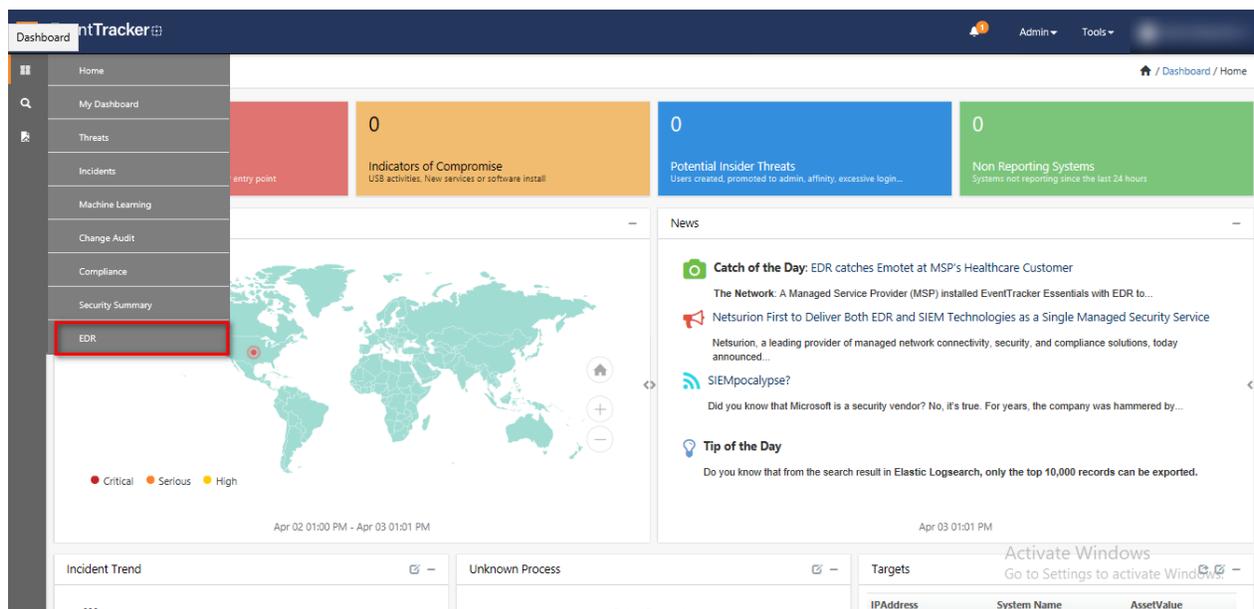


Figure 2

EventTracker EDR **Dashboard** opens (Figure 3).

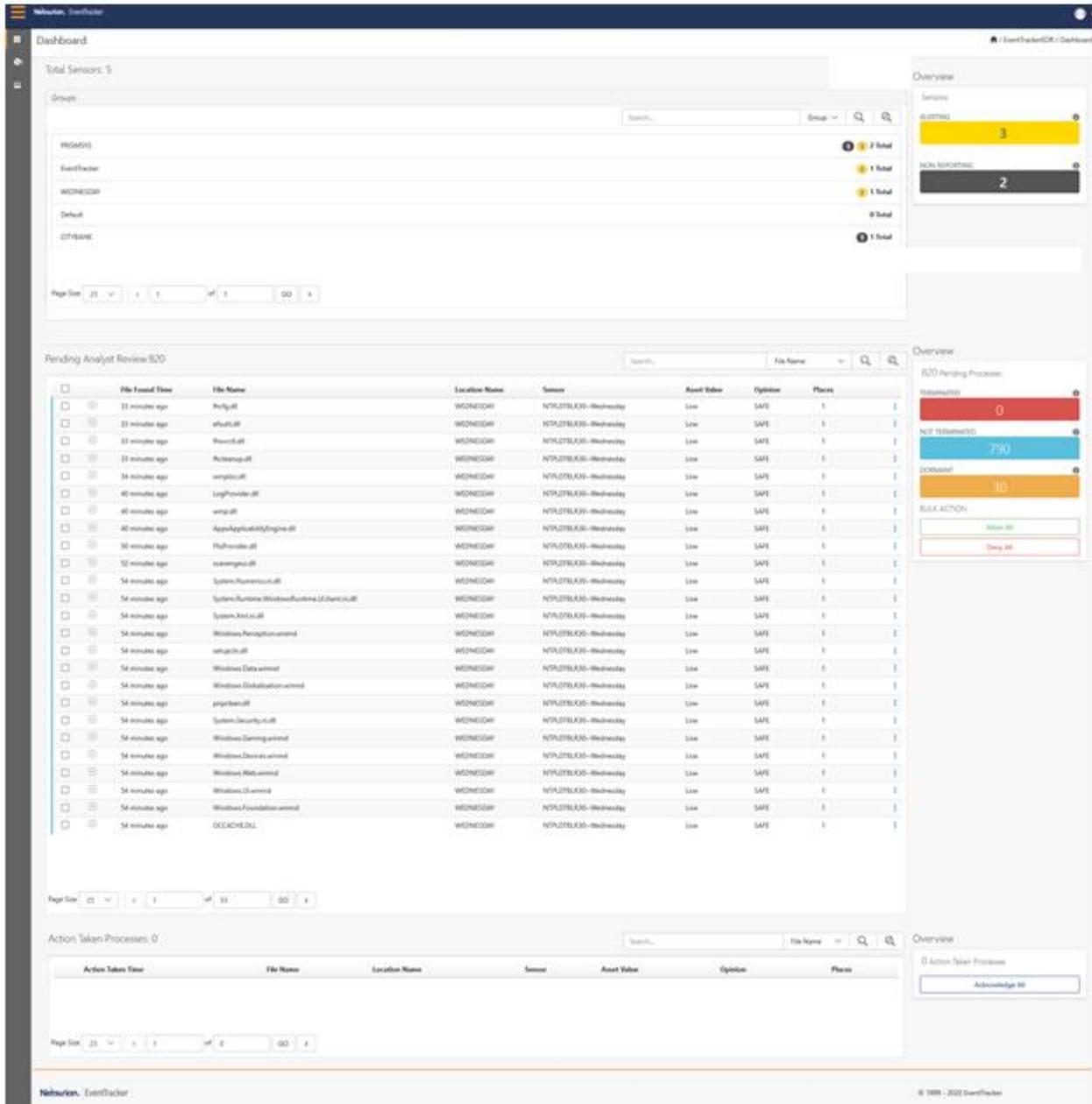


Figure 3

## 6. Dashboard

EDR sensors are installed on endpoints and configured to networks. These sensors monitor and record all system-level activities. The Dashboard displays sensor activities across all integrated devices.

The EventTracker EDR dashboard consists of three **panes** and **Overview** panels on the right.

The three panes are the following:

- **Groups pane:** In the Groups pane, by default, all the groups will be displayed in a row.
- **Pending Analyst Review pane:** This pane consists information of tracking processes, file system and registry modifications like .exe and .dll, that are to be Allowed or Denied or to be Researched.
- **Action Taken Processes pane:** This pane displays the corrective action taken (response) such as Allowed, Denied or Researched against the findings.

The three Overview panels are the following:

- The Overview panel in the Group pane: Shows the sensors/system activity status of the Group that you select.
- The Overview panel in the Pending Analyst pane: Shows the number of processes that are pending for review.
- The Overview panel in the Action Taken Processes pane: Shows the acknowledgment of all response/corrective actions taken.

The screenshot displays the EventTracker EDR dashboard. The top section, titled "Dashboard", shows "Total Sensors: 5" and a "Groups" pane with a search bar and a list of groups: "WEDNOR" (2 Total), "WEDNOR" (1 Total), "Default" (0 Total), and "OTYBAM" (1 Total). Below this is the "Pending Analyst Review 520" section, which contains a table of files. The table has columns for "File Found Time", "File Name", "Location Name", "Sensor", "Alert Value", "Option", and "Plan". The "File Found Time" column shows various times from 33 to 54 minutes ago. The "File Name" column lists various system files like "ntfs.sys", "lsass.exe", "System.Runtime.WindowsRuntime.UI.Xaml.dll", etc. The "Alert Value" column shows "Low" for all entries, and the "Option" column shows "SAFE". The "Plan" column shows "I". Below the table is the "Action Taken Processes 0" section, which is currently empty. On the right side of the dashboard, there are three "Overview" panels: "Sensors" (3), "New Suspicious" (2), and "RTO Hanging Processes" (0). The bottom right corner of the dashboard shows the copyright notice "© 1999 - 2020 EventTracker".

Figure 4

## 6.1 Groups Pane

In this pane, you will see all the Groups listed in a row, by default.

You can view events and activities of the systems/sensors through search function. The **Search** box lets you to choose **Group** or **Sensor** for viewing the status.

You can type in the name of a Group or a sensor manually in the search box to perform an individual search.



Figure 5

- Each color indicates a Group status.



Figure 6

- The status and the description are shown in the following table.

Color	Status	Description
Yellow 	ALERTING	This status shows all the locations or systems where a new process has appeared.
Gray 	NON-REPORTING	This status shows that we have not received a 'keep alive' status from there systems or locations.

- Click on the individual Group and it expands to display the sensors, and the process status of the sensors.



Figure 7

- The status and the description are shown in the following table.

Color	Status	Description
Orange 	DORMANT	Indicates the number of files detected before execution.
Red 	TERMINATED	Indicates the Terminated process by the EventTracker EDR.
Fountain Blue 	NOT TERMINATED	Indicates the process that ran during the maintenance mode and is now running without disposition.

When you click on the color icons, it filters the EDR database and displays all the events of that status in the Pending Analyst Review pane.

For example: When you click on the orange color icon, you will see all the details of the dormant processes in the Pending Analyst Review pane.



Figure 8

## 6.2 Overview of sensors in Groups Pane

The Overview of sensors provides the overall visibility of sensors in EDR deployment. It shows the status and count of incidents and events (processes).

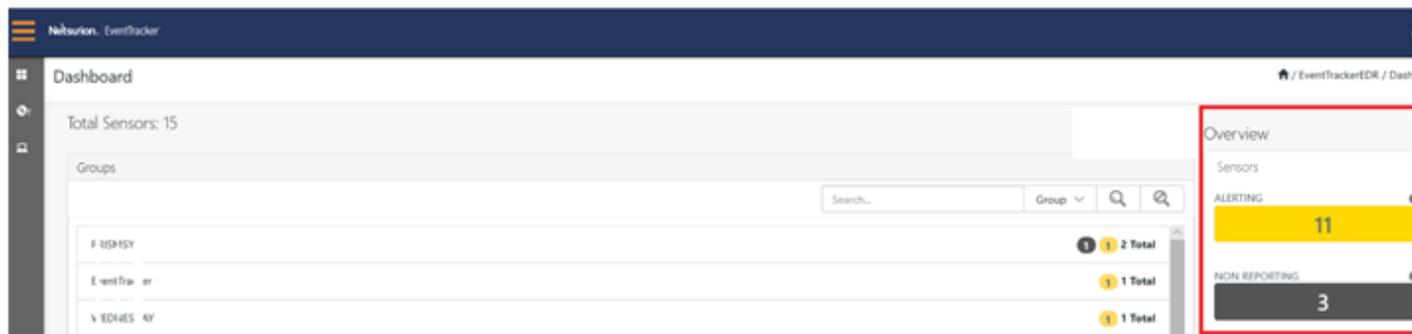


Figure 9

Color	Status	Description
Yellow <span style="background-color: yellow; border-radius: 50%; padding: 2px;">1</span>	ALERTING	This status shows all the locations or systems where a new process has appeared.
Gray <span style="background-color: gray; border-radius: 50%; padding: 2px;">1</span>	NON-REPORTING	This status shows that we have not received a 'keep alive' status from these systems or locations.

- **ALERTING:** When you click on the **Alerting** tab, you will see all the groups with Alert status listed in the Groups pane. It filters the EDR database and displays all the events of that status.

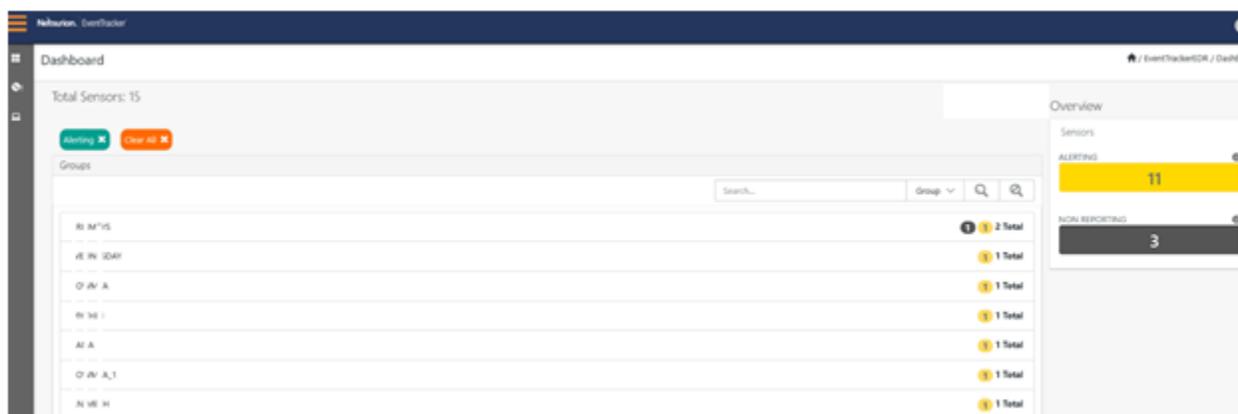


Figure 10

- **NON-REPORTING:** When you click on the **non-reporting** tab, you will see all groups with non-reporting status listed in the Groups pane. It filters the EDR database and displays all the events of that status.

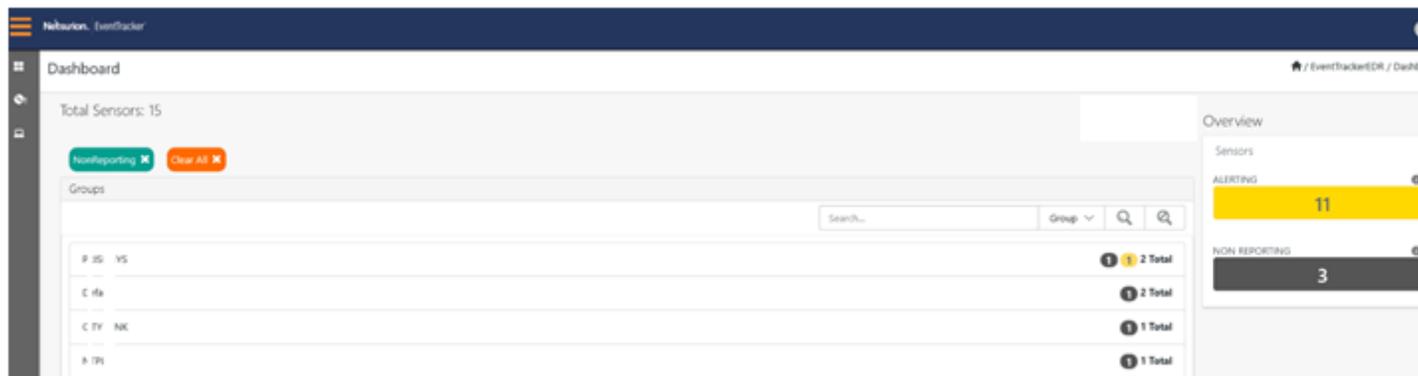


Figure 11

## 6.3 Pending Analyst Review pane

Pending Analyst Review pane consists of information about File Found Time, File Name, Location Name, Sensor, Asset Value, Opinion, and Places.

There are multiple ways to perform search from the list in the search box. The search can be done by **File Name, Sensor Name, Hash, Location, Opinion, Product Name, Signed By, File Path, Parent Process Path**.

Pending Analyst Review:10,687

File Found Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places
a minute ago	dosvc.dll	AI 5H	N 2LI B 224~f IIIMES f	Low		
a minute ago	dirct.dll	AI 5H	N 2LI B 224~f IIIMES f	Low		
2 minutes ago	mcd.sys	AI 5H	N 2LI B 224~f IIIMES f	Low		
2 minutes ago	woc.dll	AI 5H	N 2LI B 224~f IIIMES f	Low	UNKNOWN	1
4 minutes ago	uibktd.dll	AI 5H	N 2LI B 224~f IIIMES f	Low	UNKNOWN	2
6 minutes ago	A 2_1_b_0a25k2ei.dll	M HI J	ET VA 3L 22012 3~my hili	High	UNKNOWN	1

Figure 12

- You can analyze data and based on status significance you can take actions to achieve endpoint policies ranging from allow to research.
  - Data present in the Analyst pane for 3 days, without any action moves to the research pane. Action taken data moves to the action pane.
- You can do this by selecting file name in the list or by clicking the **tools**  option and choosing Allow, Deny or Research.

Pending Analyst Review:10,688

<input type="checkbox"/>	File Found Time	File Name	Location Name	Sensor	Asset Value	Opinion	
<input type="checkbox"/>	0 minutes ago	dosvc.dll	EDN^SDAY	N PLDT^R30~V^edn day	Low	UNKNOWN	<input type="button" value="Allow"/> <input type="button" value="Deny"/> <input type="button" value="Research"/>
<input type="checkbox"/>	6 minutes ago	NTL^NMA^DLL	NIME^H	N PLDT^R24~^NIMI^H	Low	UNKNOWN	1
<input type="checkbox"/>	6 minutes ago	drp:^v.dll	NIME^H	N PLDT^R24~^NIMI^H	Low	UNKNOWN	1
<input type="checkbox"/>	7 minutes ago	mrj^lav.sys	NIME^H	N PLDT^R24~^NIMI^H	Low	UNKNOWN	1
<input type="checkbox"/>	7 minutes ago	wet:^nt.dll	NIME^H	N PLDT^R24~^NIMI^H	Low	UNKNOWN	1
<input type="checkbox"/>	9 minutes ago	uirit^oon.d	NIME^H	N PLDT^R24~^NIMI^H	Low	UNKNOWN	2
<input type="checkbox"/>	11 minutes ago	Apf:^_Web_^t25k2ei.dll	YTHI^J	E^VME^t22012^3~n^thili	High	UNKNOWN	1
<input type="checkbox"/>	11 minutes ago	Apf:^_Web_^ykmiqh.dll	YTHI^J	E^VME^t22012^3~n^thili	High	UNKNOWN	1
<input type="checkbox"/>	11 minutes ago	msj:^toled^0.dll	YTHI^J	E^VME^t22012^3~n^thili	High	UNKNOWN	3
<input type="checkbox"/>	11 minutes ago	QUI^RY.DL	NIME^H	N PLDT^R24~^NIMI^H	Low	SAFE	2
<input type="checkbox"/>	12 minutes ago	Apf:^_Web_^t1puo2et.dll	YTHI^J	E^VME^t22012^3~n^thili	High	UNKNOWN	1

Figure 13

### Allowing the process

1. Click **Allow**, **Allow Process** dialog box opens.

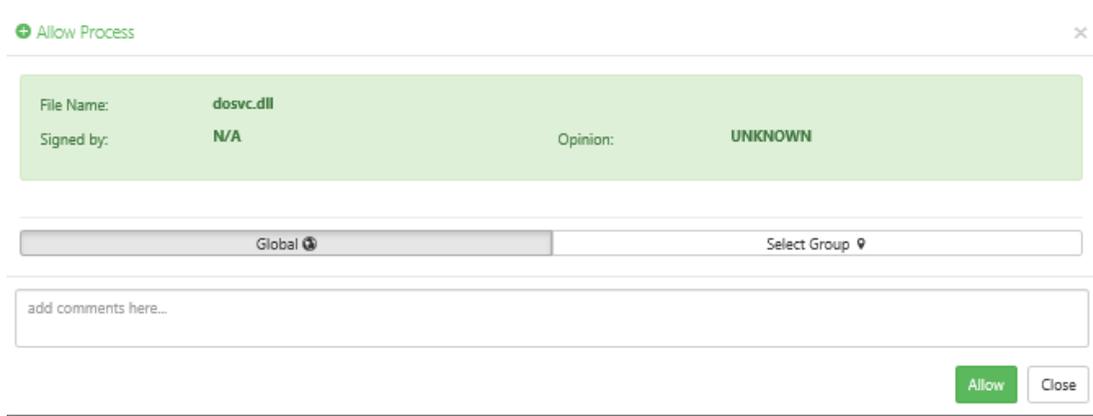


Figure 14

2. When **Global** option is selected, clicking **Allow**, selects all the groups in the environment.

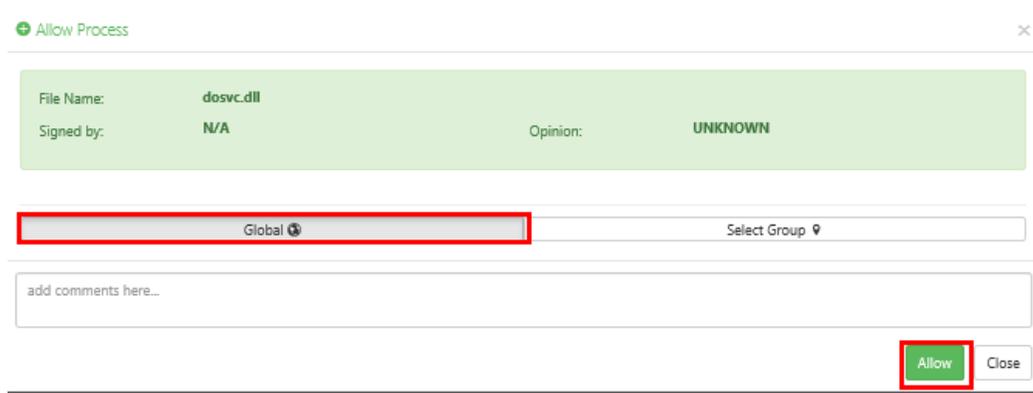


Figure 15

- When **Select Group** option is selected, clicking **Allow**, allows you to select from the Available Groups.

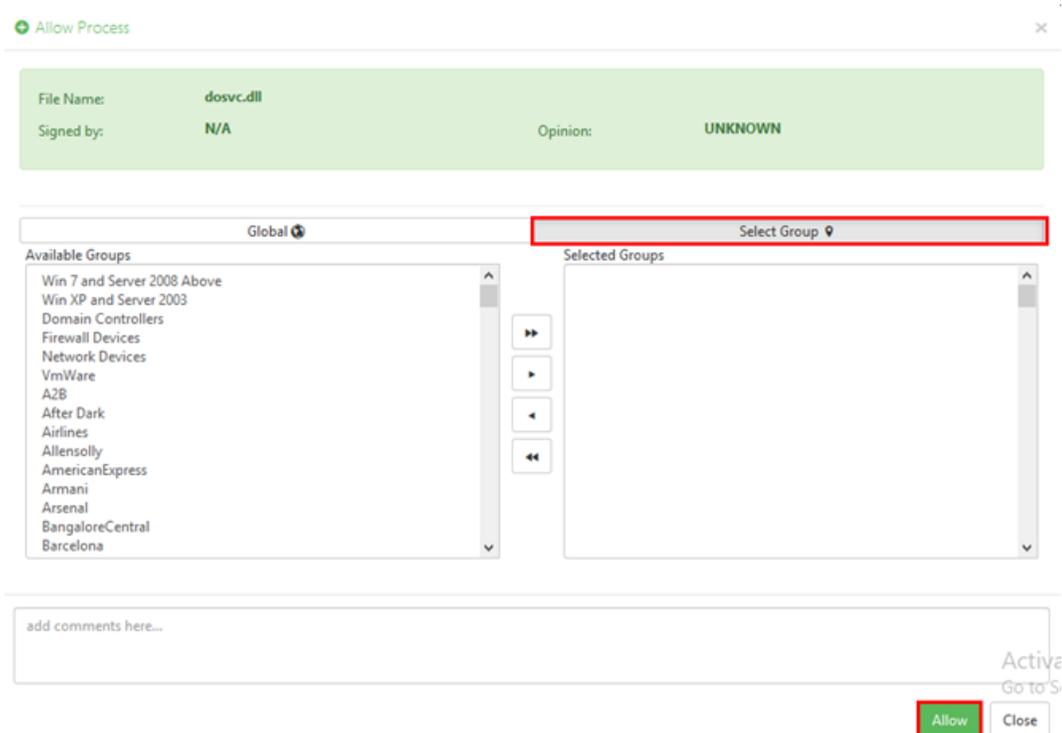


Figure 16

## Denying the process

- Click **Deny**, to open the **Deny Process** dialog box.



Figure 17

- When **Global** option is selected, clicking **Deny** will deny all the groups in the environment.

3. When **Select Group** option is selected, clicking **Deny** will deny only the selected group from the available.

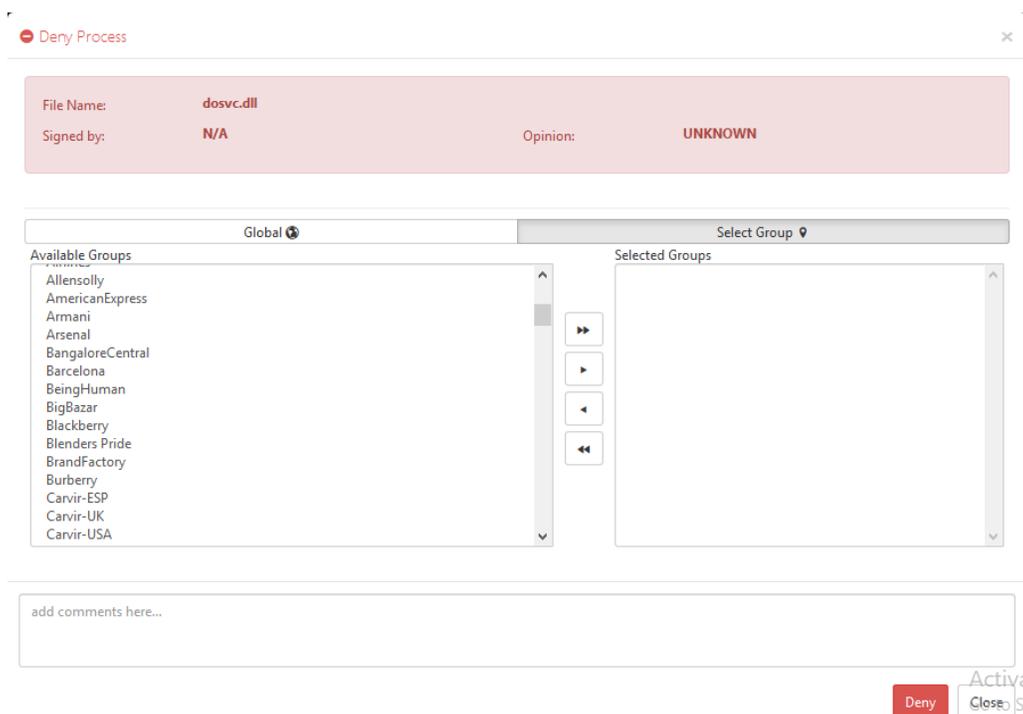


Figure 18

- Depending on the options chosen (**Allow, Deny or Research**), the respective process is displayed under the Allowed, Denied or research Category, under the Processes tab.

The Process tab is discussed in detail in the [Processes](#) Section.

**Note:** You can also search for the processes from the **Threat engines** provided by IBM XFE, Malc0de, Team Cymru.

- Click to know more about the process details.

Action Taken Processes: 29

Action Taken Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places
Mar 20 04:14:10 PM	sppsvc.exe	WEDNESDAY	NTPPLDTBLR30--Wednesday	Low	SAFE	1
Mar 20 04:14:09 PM	App_Web_un5gxqj.dll	Test_EDR	NTPPLDTBLR59--DEEPAK	Low	UNKNOWN	1
Mar 20 04:14:09 PM	App_Web_vzxiicdh.dll	Test_EDR	NTPPLDTBLR59--DEEPAK	Low	UNKNOWN	1

Overview  
29 Action Taken Processes  
Acknowledge All

Figure 19

The Pending Analyst Review screen opens. If you want to allow, deny, or research the process, choose the appropriate option.

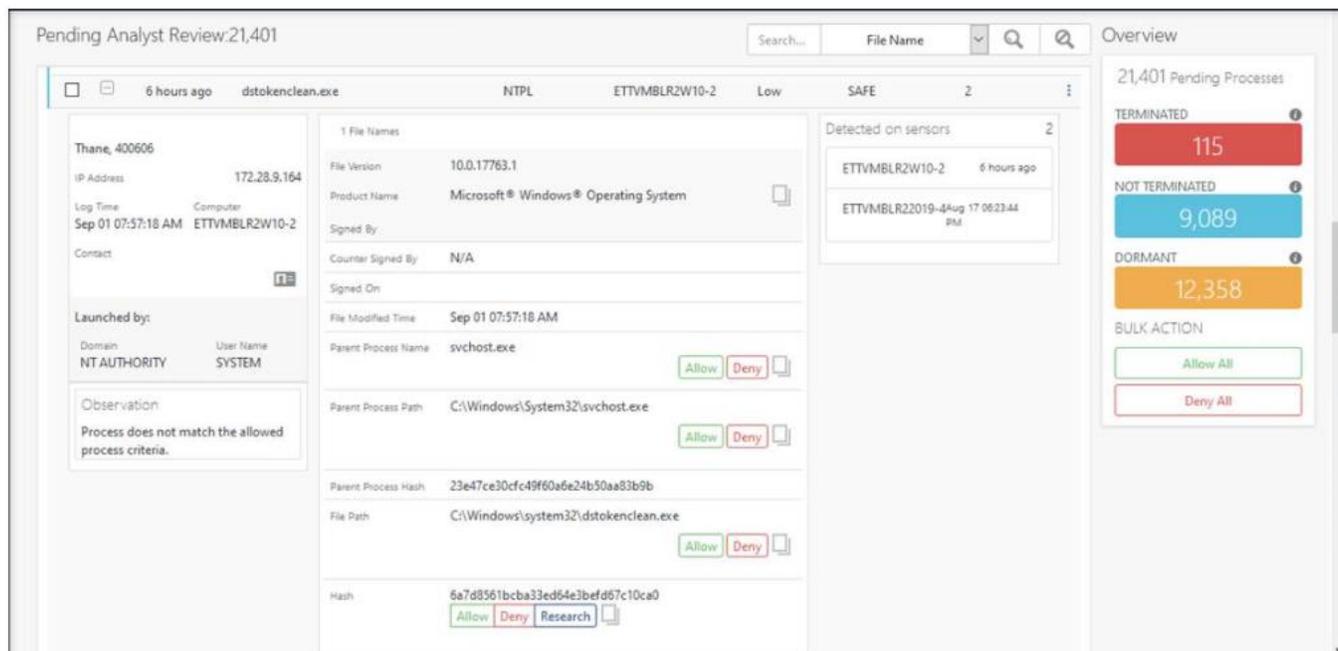


Figure 20

User can allow/deny a process through four different approaches.

1. Parent process name – used when you want to allow/deny by parent process name.
2. Parent process path – used when you want to allow/deny by parent process path.
3. File path – used when you want to allow/deny by file path.
4. Hash – used when you want to allow/deny by hash.

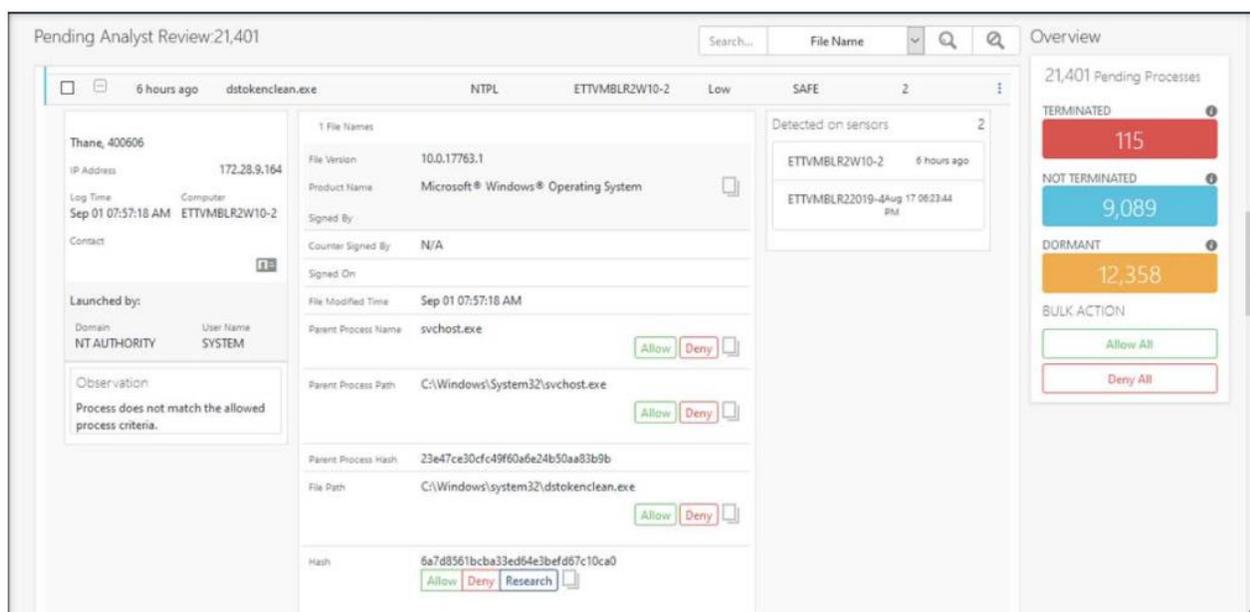


Figure 21

**NOTE:**

If w3wp.exe process is allowed along with the parent process name, then in future if w3wp.exe process is detected with the same parent process name, it will be automatically considered as safe.

In the latest version of EventTracker v9.3, we have introduced the option to allow/deny a process name by including parent process hash.

If w3wp.exe process is allowed along with the parent process name and parent process hash value (E.g. abc), then in future if w3wp.exe process is detected with a different parent process hash value (E.g. xyz) it will not be considered as safe. User needs to take appropriate action (allow/deny) again.

Pending Analyst Review:12,589

Search... File Name

Overview

12,589 Pending Processes

TERMINATED 93

NOT TERMINATED 251

DORMANT 12,250

BULK ACTION

Allow All

Deny All

1 File Names

File Version 0.0.0.0

Product Name

Signed By

Counter Signed By N/A

Signed On

File Modified Time Sep 04 10:30:54 AM

Parent Process Name w3wp.exe

Parent Process Path C:\Windows\SysWOW64\inetmgr\w3wp.exe

Parent Process Hash 3c49492762be5985185665a7202c4dda

File Path C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files\eventtracker\29c5a12a\b40dd6bb\App\_Web\_jzh5vixid.dll

Hash f92b34b8bc281a87b43c93d1b0bcdc1e

Observed on sensors 1

ETTVMBLR22019-4 1 hours ago

1 hours ago App\_Web\_jzh5vixid.dll EventTracker ETTVMBLR22019-4 Serious UNKNOWN 1

Thane, 400606

IP Address 172.28.9.147

Log Time Sep 04 10:30:54 AM

Computer ETTVMBLR22019-4

Contact

Launched by:

Domain User Name

NT AUTHORITY NETWORK SERVICE

Observation

Process loaded a binary that does not match the allowed criteria.

Figure 22

Clicking **Allow** on Parent process name will fetch Parent process hash value in the **Add rule** window.

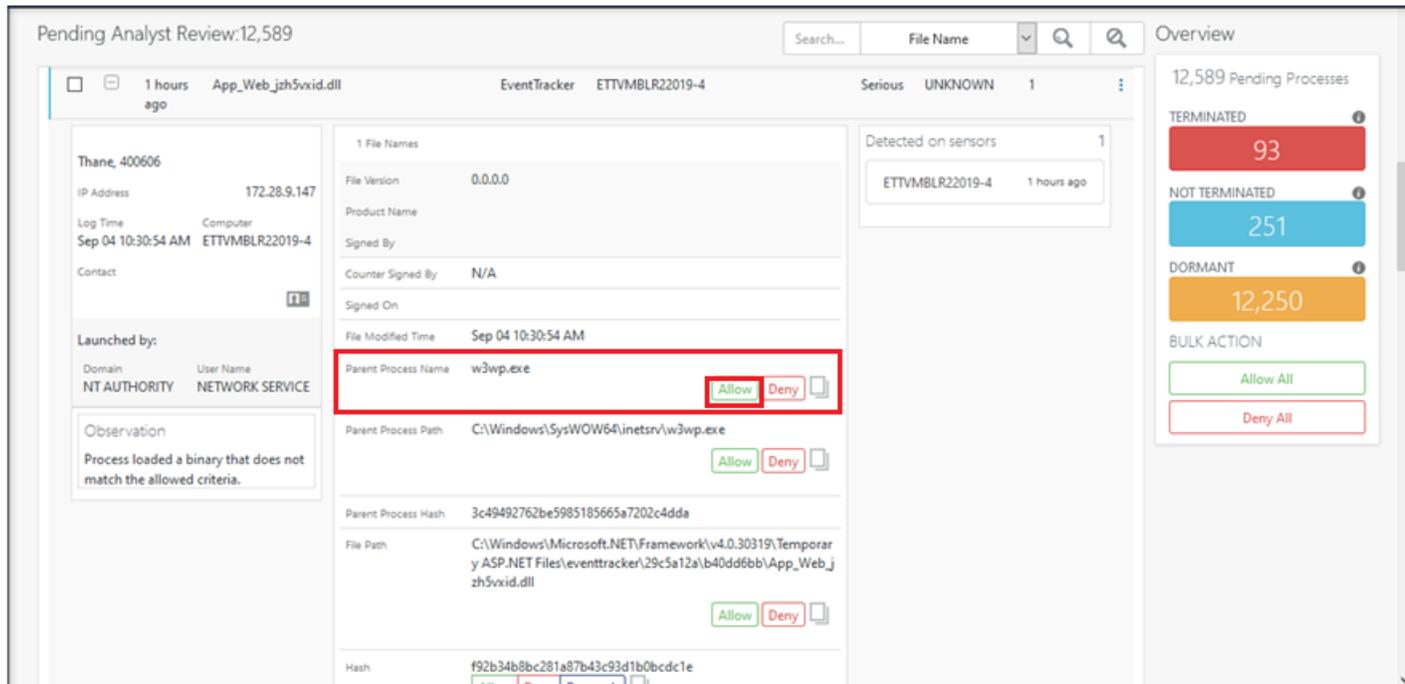


Figure 23

Add rule window

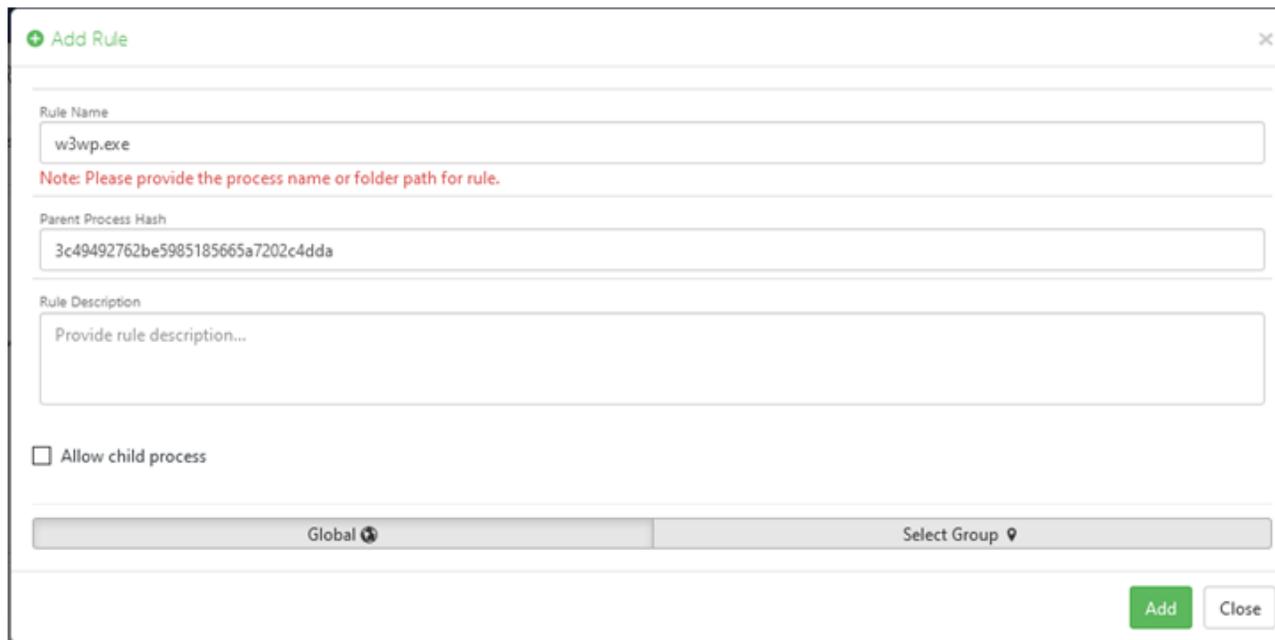


Figure 24

If the user removes the Parent Process Hash value, then any process with the same process name is considered safe.

## 6.4 Overview of the Pending Processes

The Overview panel provides the overall visibility of processes in EDR deployment that are **Terminated**, **Non-terminated** and **Dormant**.

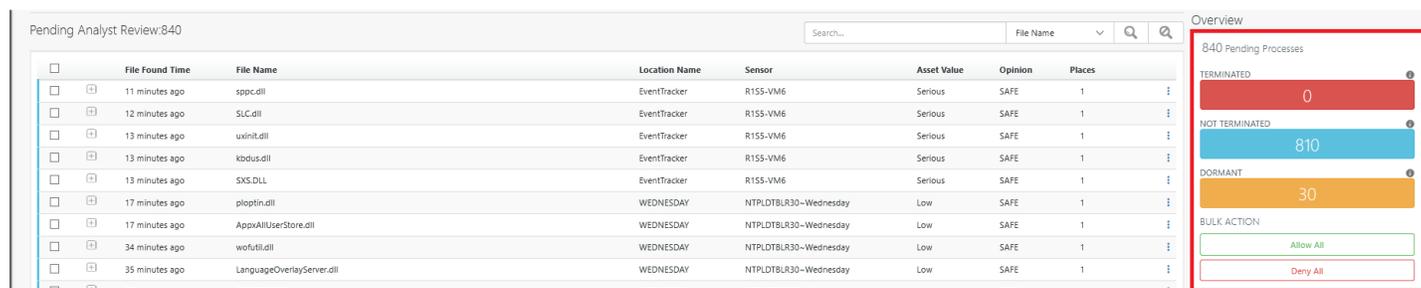


Figure 25

- The status and the description are shown in the following table.

Color	Status	Description
Red <span style="color: red; font-weight: bold;">0</span>	TERMINATED	Indicates the Terminated process by the EventTracker EDR.
Fountain Blue <span style="color: blue; font-weight: bold;">0</span>	NOT-TERMINATED	Indicates the process that ran during the maintenance mode and is now running without disposition.
Orange <span style="color: orange; font-weight: bold;">0</span>	DORMANT	Indicates the number of files detected before execution.

- TERMINATE:** When you click on the **TERMINATE** tab, you will see all the terminated process listed in the Analyst Review pane. It filters the EDR database and displays all the events of that status.

Terminated ✕ Clear All ✕

Pending Analyst Review: 0

File Found Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places
-----------------	-----------	---------------	--------	-------------	---------	--------

Page Size: 25 < 1 of 0 GO >

Action Taken Processes: 0

Action Taken Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places
-------------------	-----------	---------------	--------	-------------	---------	--------

Overview

463 Pending Processes

TERMINATED 0

NOT TERMINATED 463

DORMANT 0

BULK ACTION

Allow All Deny All

Acknowledge All

Figure 26

- **NOT TERMINATED:** When you click on the **NON-TERMINATED** tab, you will see all the non-terminated processes listed in the Analyst Review pane. It filters the EDR database and displays all the events of that status.

Not terminated ✕

Pending Analyst Review: 810

	File Found Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places
<input type="checkbox"/>	4 minutes ago	NOTEPAD.EXE	EventTracker	R1SS-VM6	Serious	SAFE	1
<input type="checkbox"/>	41 minutes ago	System.Runtime.ni.dll	EventTracker	R1SS-VM6	Serious	SAFE	1
<input type="checkbox"/>	1 hours ago	sppc.dll	EventTracker	R1SS-VM6	Serious	SAFE	1
<input type="checkbox"/>	1 hours ago	SLC.dll	EventTracker	R1SS-VM6	Serious	SAFE	1
<input type="checkbox"/>	1 hours ago	uxinit.dll	EventTracker	R1SS-VM6	Serious	SAFE	1
<input type="checkbox"/>	1 hours ago	kbdus.dll	EventTracker	R1SS-VM6	Serious	SAFE	1
<input type="checkbox"/>	1 hours ago	SXS.DLL	EventTracker	R1SS-VM6	Serious	SAFE	1
<input type="checkbox"/>	1 hours ago	plpfin.dll	WEDNESDAY	NTPRLTBLR30-Wednesday	Low	SAFE	1

Overview

840 Pending Processes

TERMINATED 0

NOT TERMINATED 810

DORMANT 30

BULK ACTION

Allow All Deny All

Figure 27

- **DORMANT:** When you click on the **DORMANT** tab, you will see all the dormant processes listed in the Analyst Review pane. It filters the EDR database and displays all the events of that status.

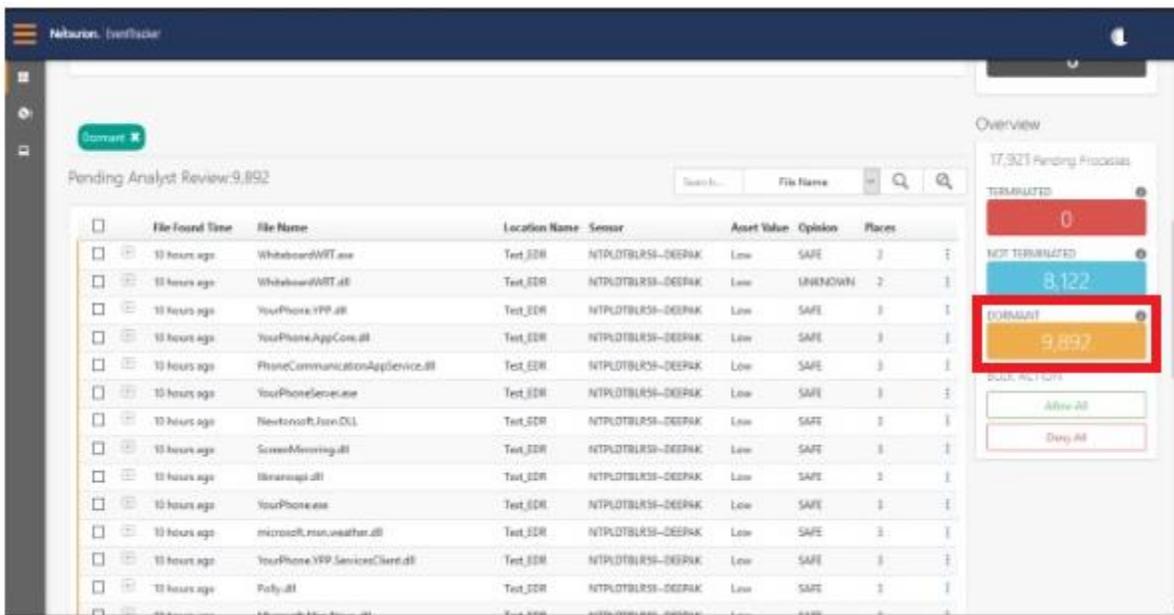


Figure 28

Clicking on **Allow All** button under the **Bulk Action** will let all the processes to be allowed, which can be viewed in the **Allowed Process** option in the **Process tab**.

Similarly, clicking on **Deny All** button under the **Bulk Action** will deny all the processes and it can be viewed in the **Denied Process** option in the **Process tab**.



Figure 29

To select the individual process, click the check box as shown in the following figure

In the Bulk Action window, click **Allow Selected** to allow the process and click **Deny selected** to deny the selected process.

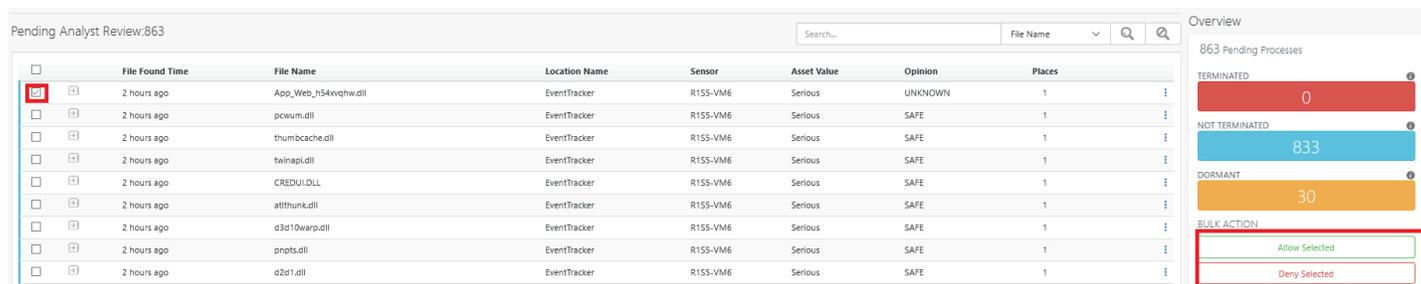


Figure 30

## 6.5 Action Taken Processes Pane

There are multiple ways to perform search from the list in the search box. The search is done by **File Name, Sensor Name, Hash, Location, Opinion, Product Name, Signed By, File Path, Parent Process Path, Parent Process Name, Parent Process Hash.**

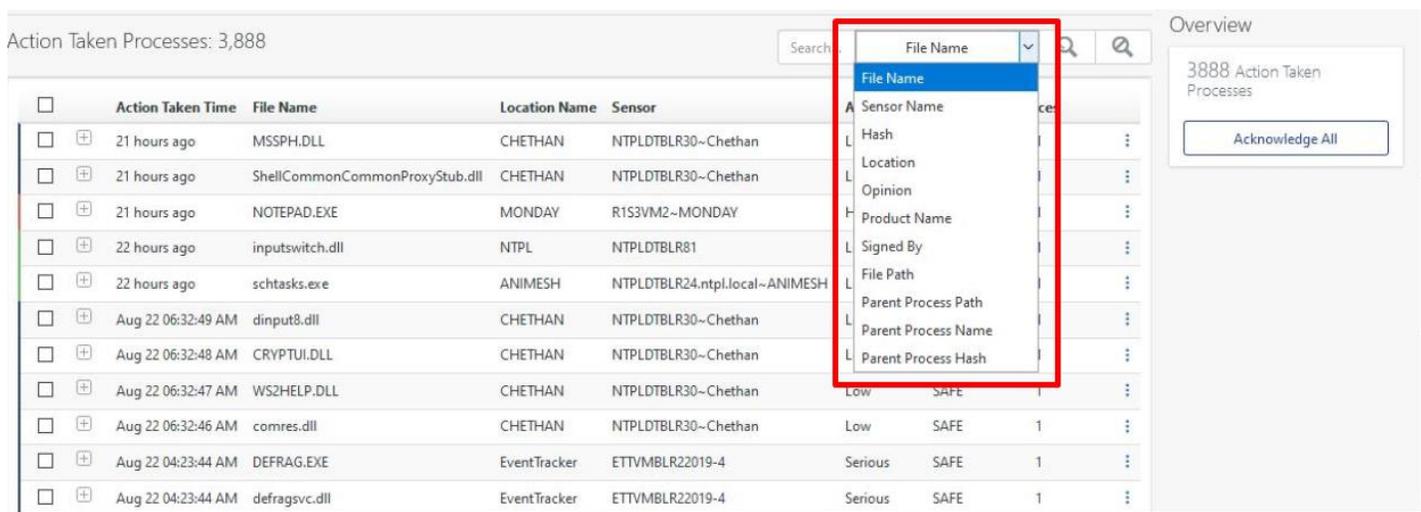


Figure 31

1. Click on the icon to expand the tab. You will see the detailed information about the File Names and the corrective action taken.

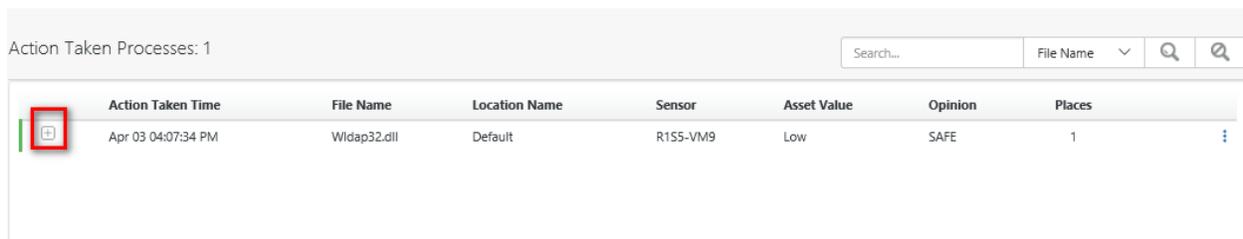


Figure 32

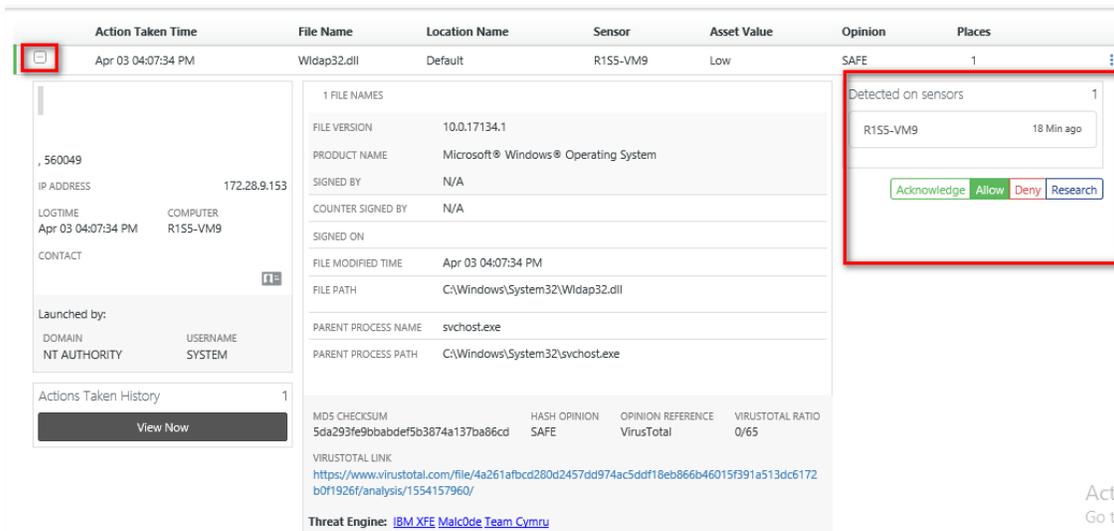


Figure 33

- You can do a further investigation and can choose to **Deny** or **Research** the process from the Action Taken processes window, by clicking on the  settings icon in the upper-right corner.

Click **View Now** will show the **Action taken history** of the user and the comments, if provided by the users.

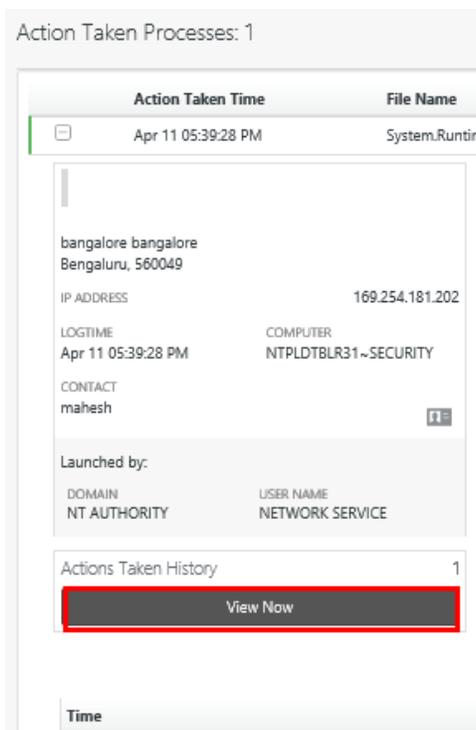


Figure 34

Time	Action Taken	Group(s)	User	Comments
Mar 13 06:20:24 PM	Allowed	1 Groups	s ktir p	

Figure 35

## 6.6 Overview of the Action Taken Processes

Click **Acknowledge All**, to acknowledge all the processes in the **Action Taken** Process tab. The acknowledged processes can be viewed on the Process page, under the allowed process or denied process, based on the action.

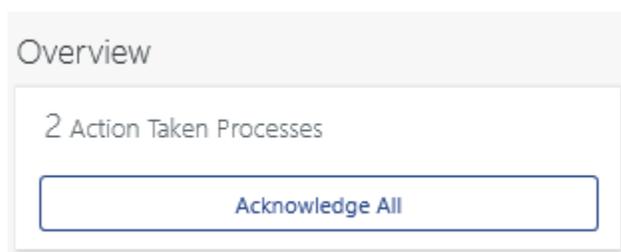


Figure 36

## 7. Processes page

In process page you can check process vendor and rule of an sensors

On the left Ribbon, click **Processes** Icon  to navigate to the Processes page.

The screenshot shows the 'Processes' page in the Netsurion EventTracker interface. The left sidebar has a 'Processes' icon highlighted. The main content area displays summary statistics:

- Vendors: 66,270
- Collections: 4
- Approved Vendors: 34
- Rules: Allowed Rules 0, Denied Rules 0
- Allowed Process: 2,097,495
- Denied Process: 2
- Research Process: 0

An 'Overview' panel on the right shows a bar chart with three categories: ALLOWED (2,097,495), DENIED (2), and RESEARCH (0).

Figure 37

The processes page will have the following:

- **Vendors**
- **Rules**
- **Allowed Process**
- **Denied Process**
- **Research Process**

The Overview of the processes is displayed in the right pane.

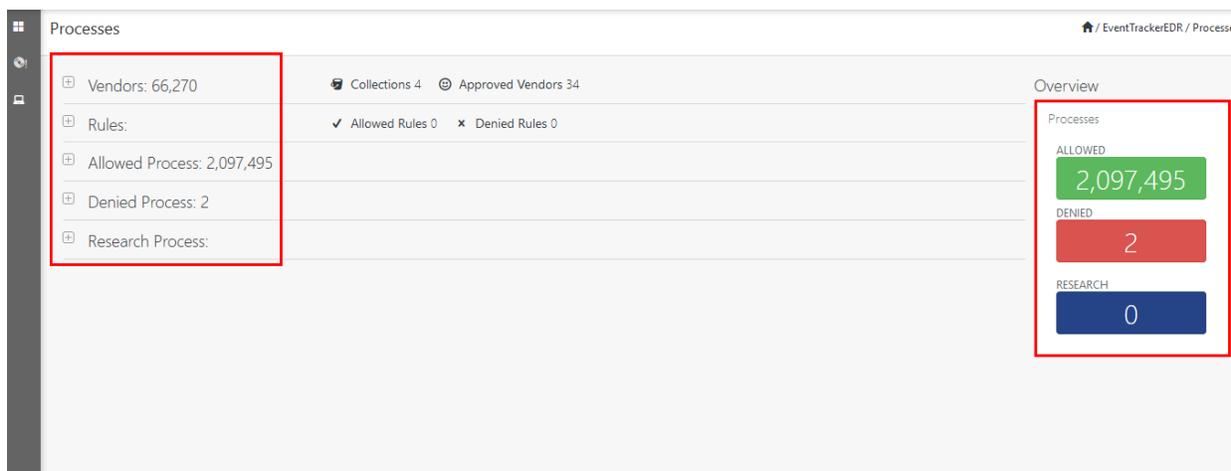


Figure 38

In the Overview panel you can view the number of processes that are **ALLOWED, DENIED AND RESEARCHED**.

Color	Processes	Description
Green	ALLOWED	The number of processes that were Allowed.
Red	DENIED	The number of processes that were Denied.
Blue	RESEARCH	The number of processes that were Researched.

## 7.1 Vendors

- Click  icon on the vendor's tab.

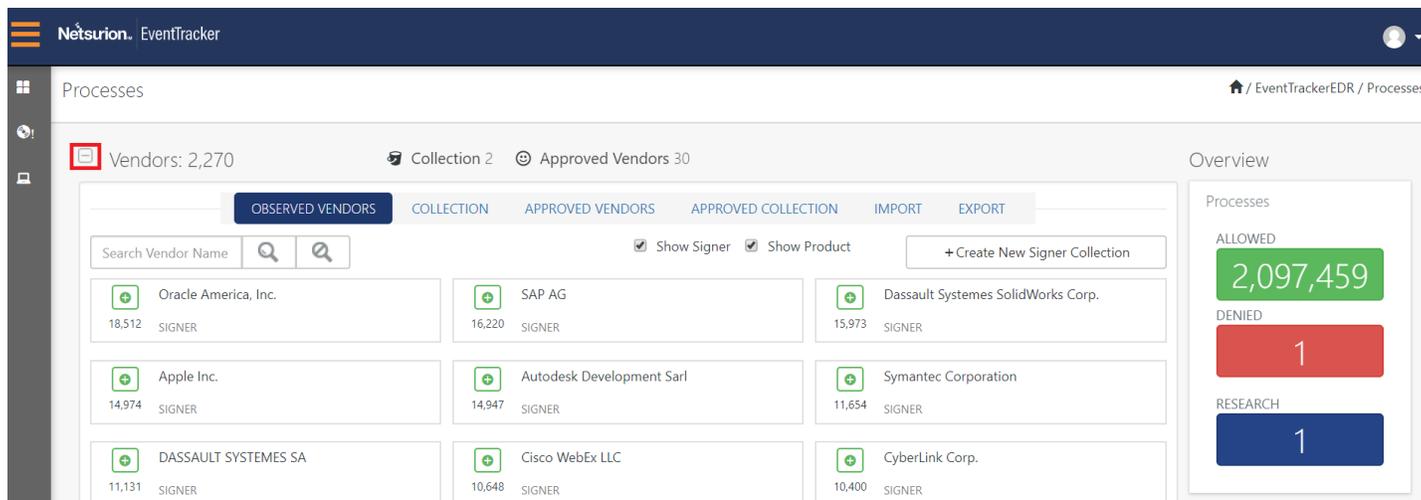


Figure 39

The Vendors page opens with the following tabs

- **OBSERVED VENDORS**
- **COLLECTION**
- **APPROVED VENDORS**
- **APPROVED COLLECTION**
- **IMPORT**
- **EXPORT**

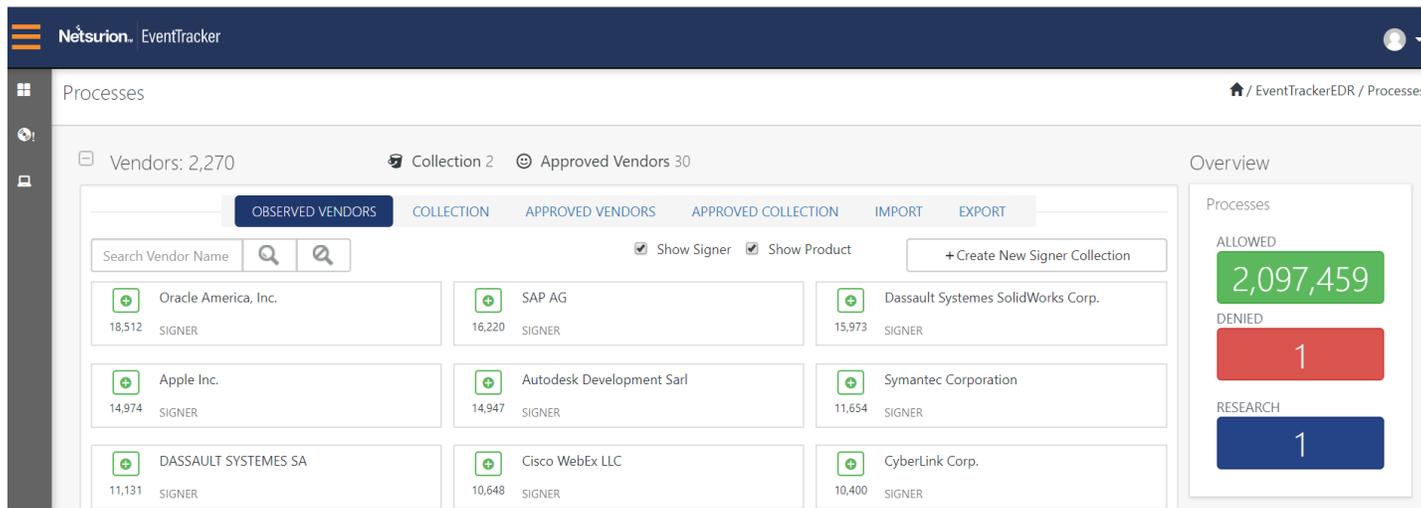


Figure 40

### 7.1.1 Observed Vendors

- It displays all the vendors present in the environment.

The screenshot shows the Netsurion EventTracker interface for 'Processes'. The 'Observed Vendors' tab is selected, displaying a grid of vendor cards. The 'Show Signer' checkbox is checked, and the 'Show Product' checkbox is unchecked. The 'Overview' panel on the right shows 2,097,459 Allowed, 1 Denied, and 1 Research items.

Vendor Name	Count	Status
Oracle America, Inc.	18,512	SIGNER
SAP AG	16,220	SIGNER
Dassault Systemes SolidWorks Corp.	15,973	SIGNER
Apple Inc.	14,974	SIGNER
Autodesk Development Sarl	14,947	SIGNER
Symantec Corporation	11,654	SIGNER
DASSAULT SYSTEMES SA	11,131	SIGNER
Cisco WebEx LLC	10,648	SIGNER
CyberLink Corp.	10,400	SIGNER

Figure 41

- You can view or search vendors based on Signer or Product Vendors. When you select **Show Signer**, you can view only the Signer Vendors.

The screenshot shows the Netsurion EventTracker interface for 'Processes'. The 'Observed Vendors' tab is selected, displaying a grid of vendor cards. The 'Show Signer' checkbox is checked, and the 'Show Product' checkbox is unchecked. The 'Overview' panel on the right shows 2,097,459 Allowed, 1 Denied, and 1 Research items.

Vendor Name	Count	Status
Oracle America, Inc.	18,512	SIGNER
SAP AG	16,220	SIGNER
Dassault Systemes SolidWorks Corp.	15,973	SIGNER
Apple Inc.	14,974	SIGNER
Autodesk Development Sarl	14,947	SIGNER
Symantec Corporation	11,655	SIGNER
DASSAULT SYSTEMES SA	11,131	SIGNER
Cisco WebEx LLC	10,648	SIGNER
CyberLink Corp.	10,400	SIGNER

Figure 42

- When you select **Show Product**, you can view only the Product Vendors.

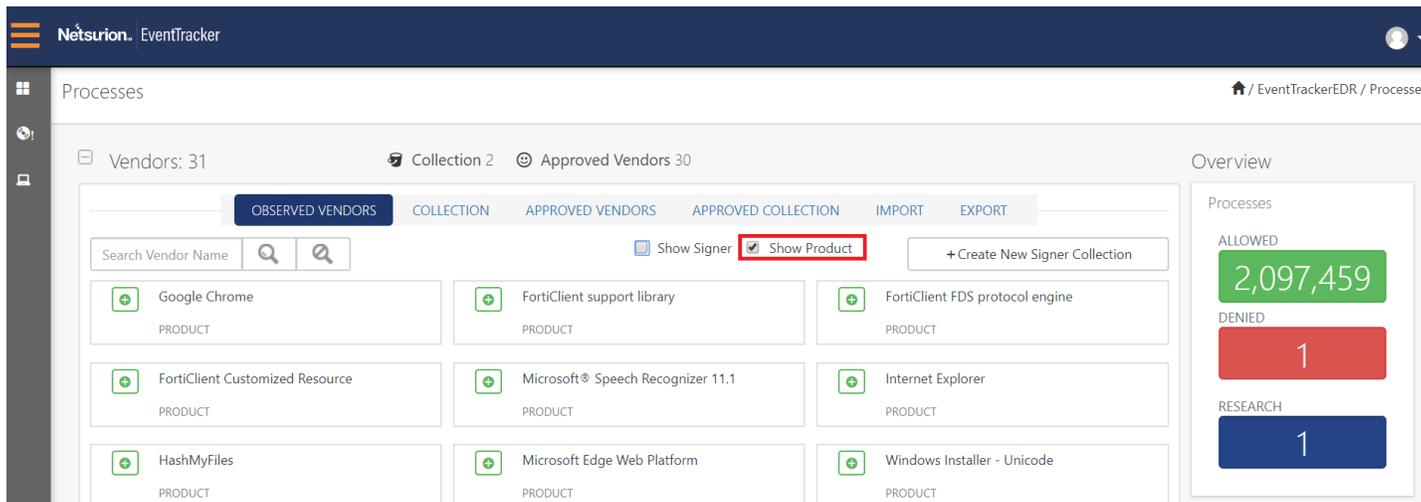


Figure 43

- When you select both the options, you can view both Signer and Product vendors.

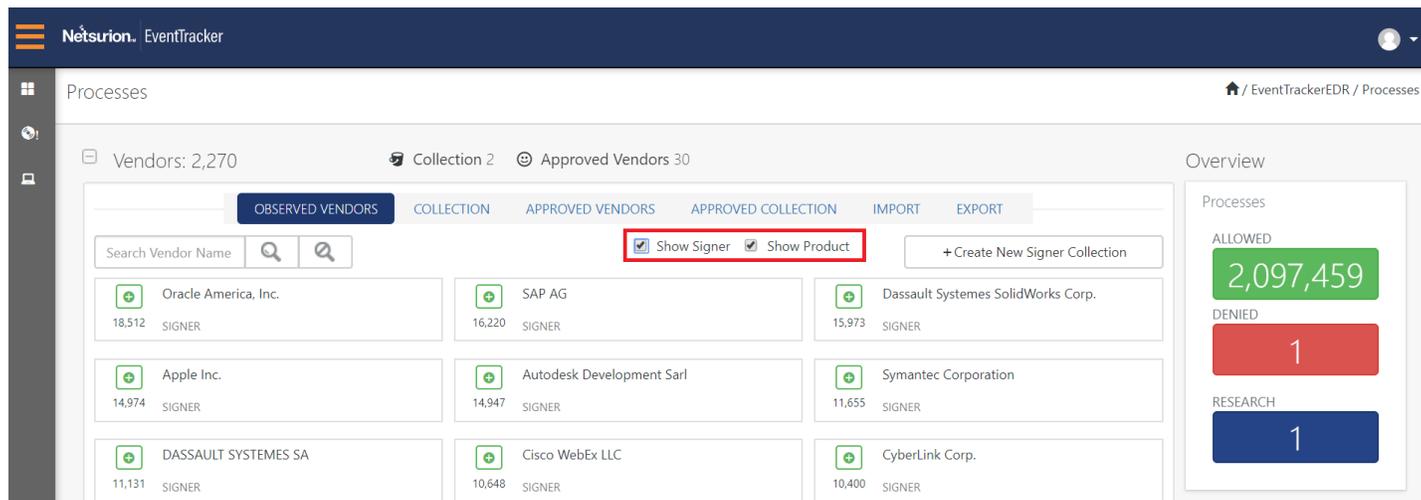


Figure 44

- Click **+ Create New Signer Collection** tab to create new vendors and edit vendor groups.

The screenshot shows the Netsurion EventTracker interface. The main content area is titled 'Processes' and displays a grid of vendor cards under the 'Vendors: 2,270' tab. The grid is organized into three columns and three rows. Each card shows a vendor name, a green plus icon, and a 'SIGNER' status. A red box highlights the '+ Create New Signer Collection' button in the top right corner of the grid. The interface also includes a search bar, a sidebar with navigation icons, and an 'Overview' panel on the right showing process statistics: ALLOWED (2,097,459), DENIED (1), and RESEARCH (1).

Figure 45

To create or edit vendor group:

1. Click **+ Create New Signer Collection** tab and **Add Vendor Collection** window opens.
2. Type the vendor name in the **Vendor Collection Name** box.
3. Click **Save**.

You can also create or add vendors from **Available Vendor** list.

The screenshot shows the 'Add Vendor Collection' dialog box. The 'Vendor Collection Name' field is highlighted with a red box and contains the text 'Test'. Below the field are two lists: 'Available Vendor' and 'Selected Vendor'. The 'Available Vendor' list contains several items, including 'Antir3.Runtime', 'Beyond Compare', 'Clip', 'EventTracker', 'FortiClient Auto-update A', 'FortiClient Customized Re', 'FortiClient FDS protocol', and 'FortiClient support libra'. The 'Selected Vendor' list is currently empty. A red box highlights the 'Save' button at the bottom right of the dialog.

Figure 46

1. Select the vendors from the available list and then **click**  icon.
2. The selected vendors will be added to the **Selected Vendor** list.
3. Select  icon to select multiple vendors at a time.
4. Click **Save**.

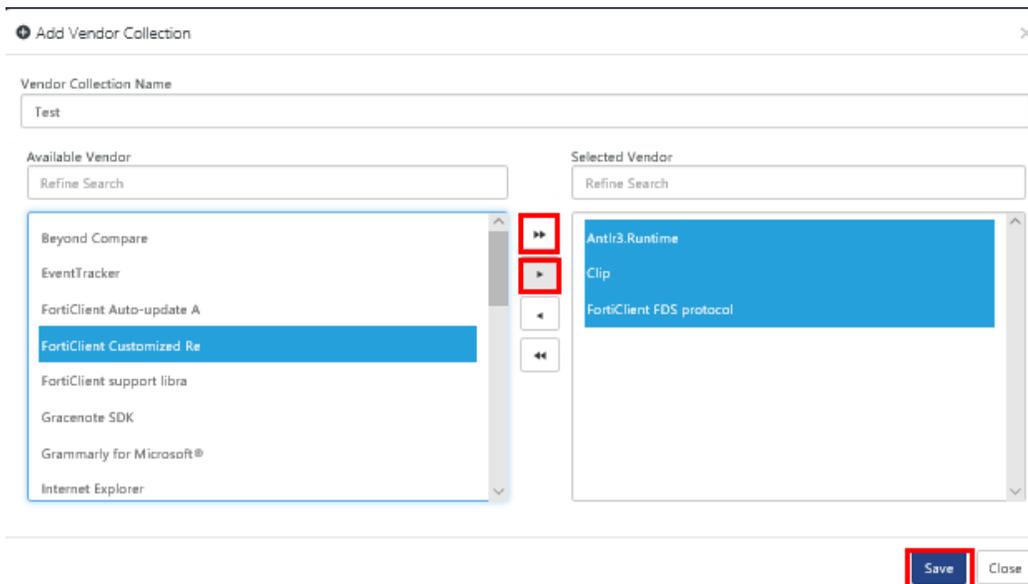


Figure 47

- You can also manually search for the **vendors** from the available list by typing in the **search box**.

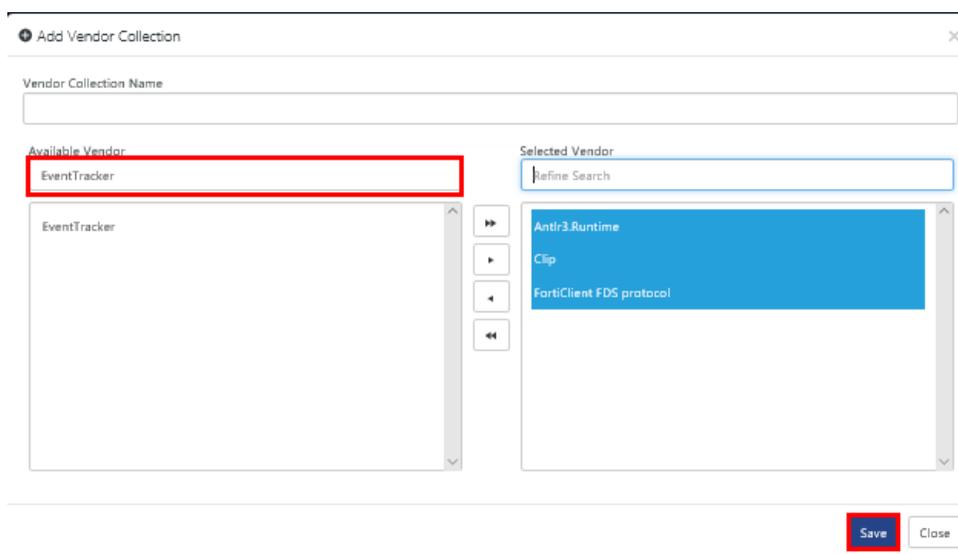


Figure 48

1. To unselect the vendors from collection, click  icon in the Selected Vendor list.
2. To unselect multiple vendors, click  icon.
3. Click **Save**.

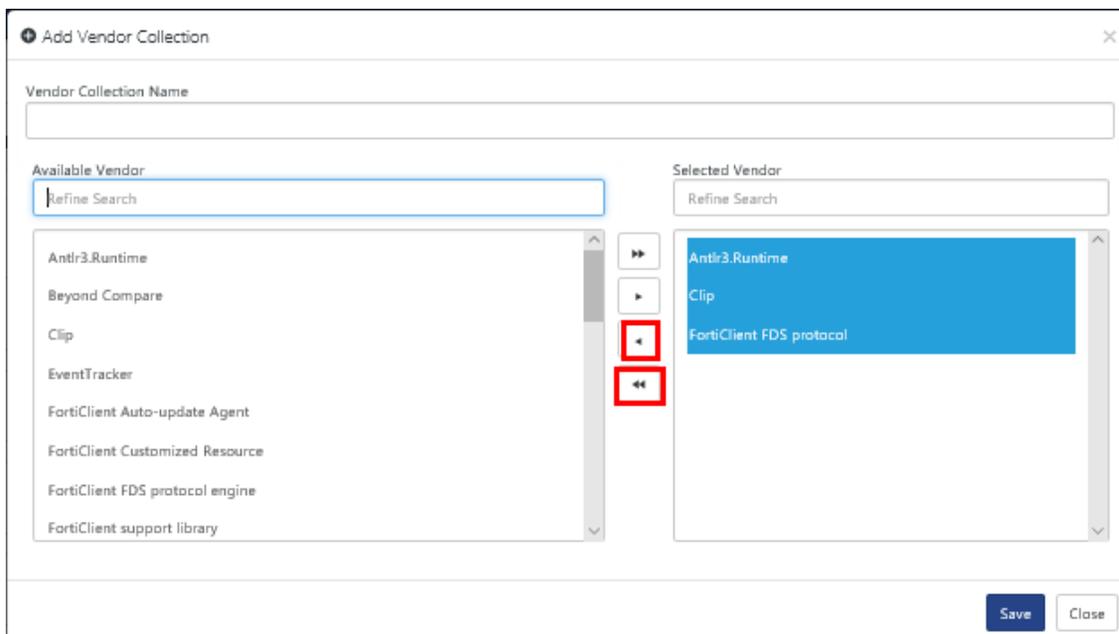


Figure 49

### 7.1.2 Collection

1. Click the **COLLECTION** tab, to view the vendor groups.

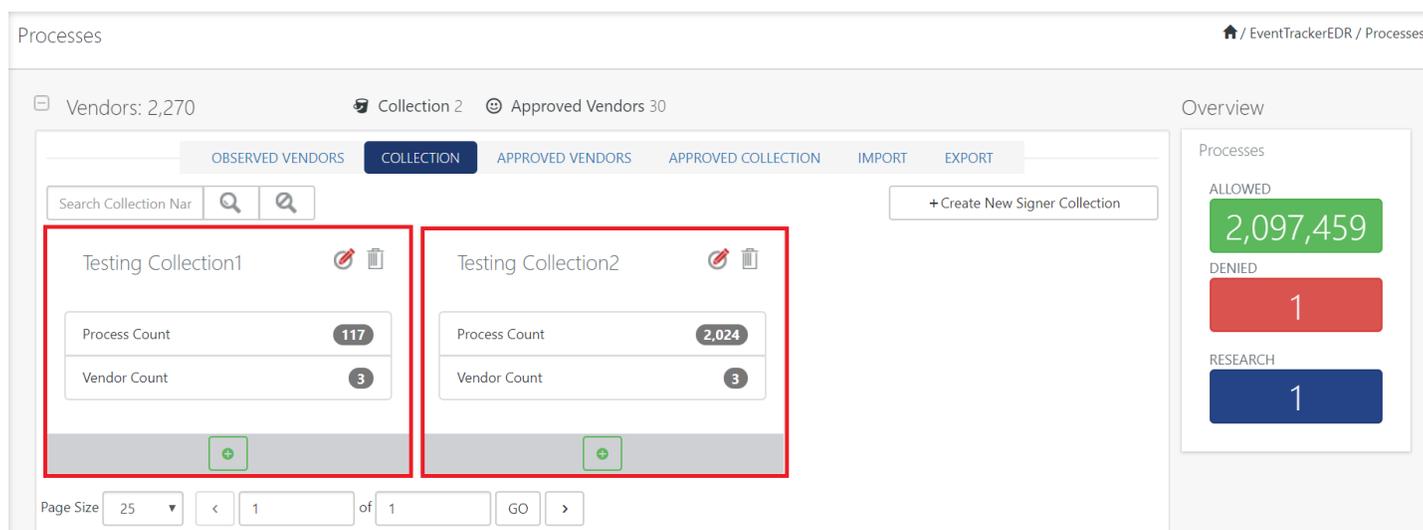


Figure 50

2. Click **Edit**  to edit the Vendor Collection, in the **Edit Vendor Collection** Window.
3. In the **Selected Vendor** section, three vendors are listed, as a result, number 3 is displayed in the Vendor Count in the above figure.
4. The **Process Count** displays the total number of processes in the Test group.

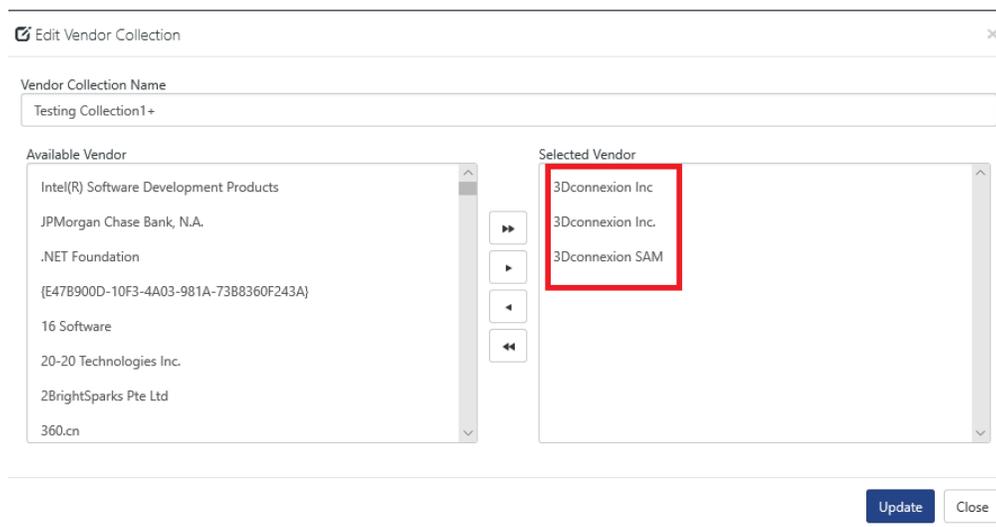


Figure 51

5. If any modifications are done to the **Vendor Collection Name** or **Selected Vendor**, you may select **Update** or click **Close**.

### 7.1.3 Approved Vendors

- Click the **APPROVED VENDORS** tab to view the list of Approved Vendors.

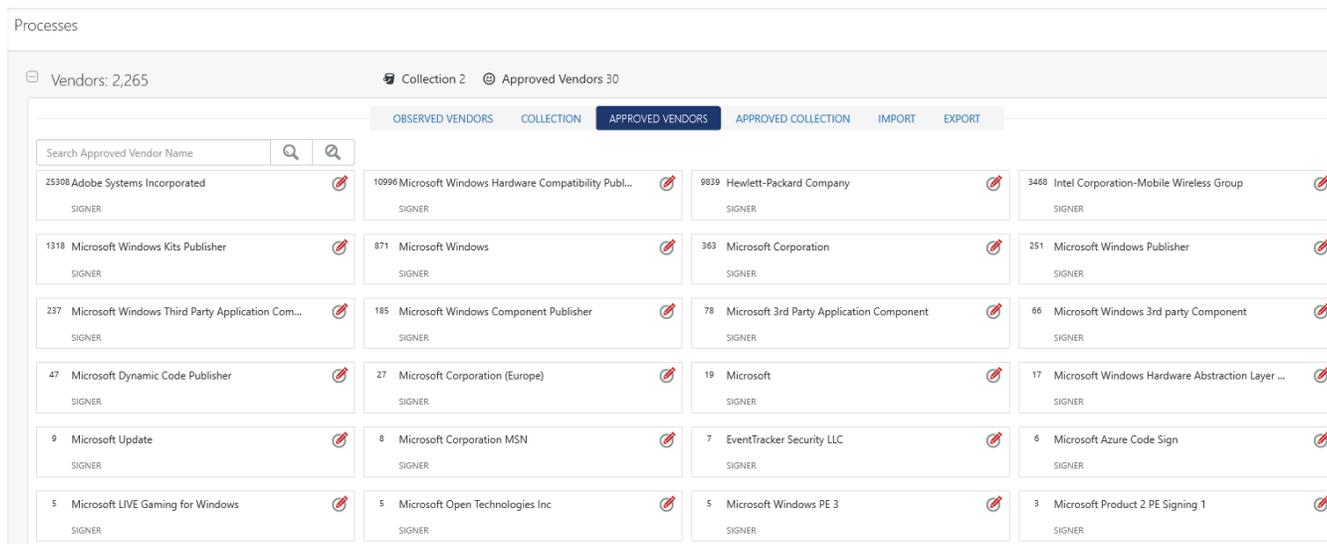


Figure 52

### 7.1.4 Approved Collection

- Click the **APPROVED COLLECTION** tab to view the list of Approved Vendors Collection.

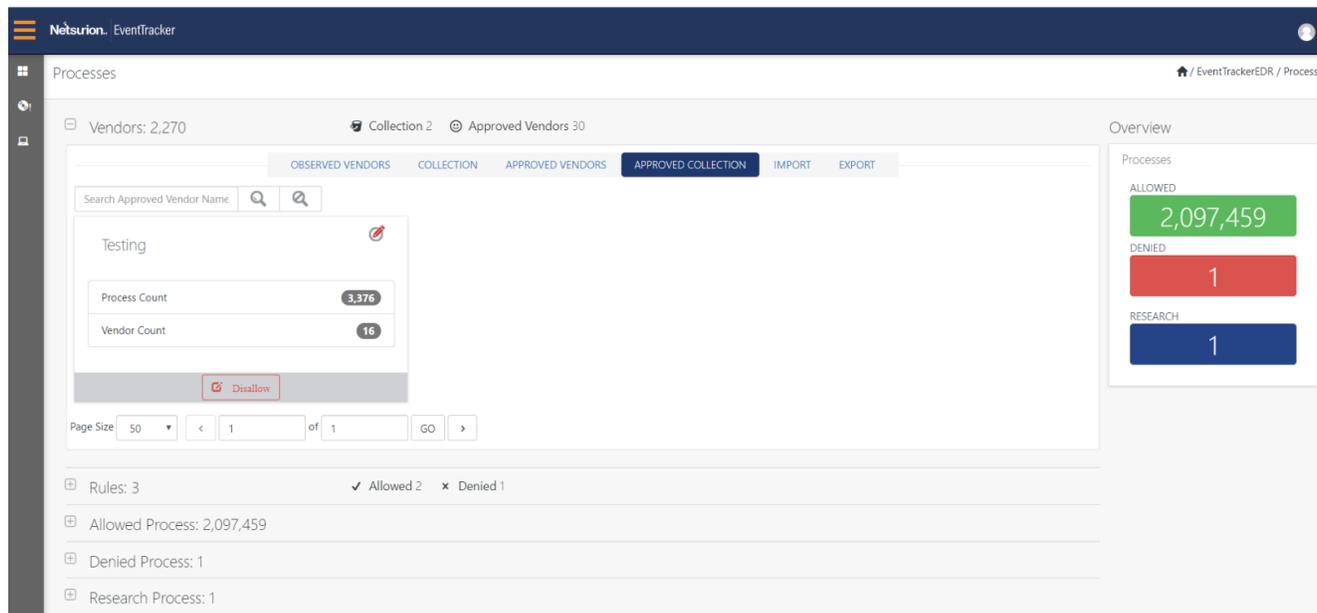


Figure 53

- As the Create New Signer Collection from the collection tab is approved, the collection is displayed in the **Approved Collection** tab.
- In the following figure, **Testing Collection1** is a Vendor Group.

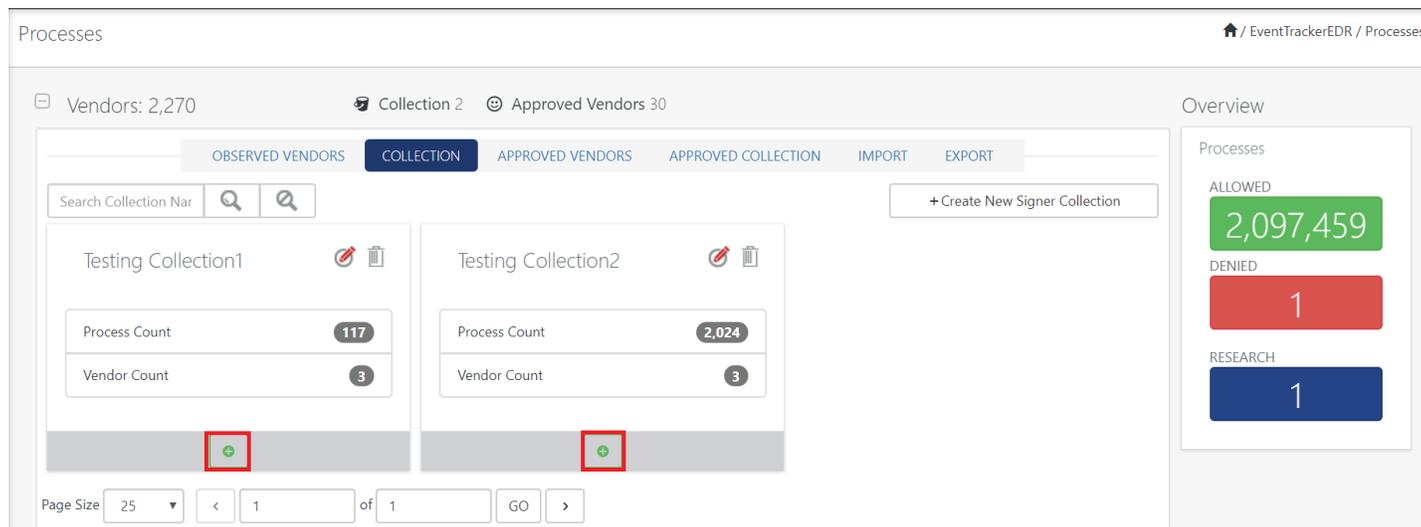


Figure 54

1. Click  icon present on the respective vendors to open the **Allow Vendor Collection** dialog box.

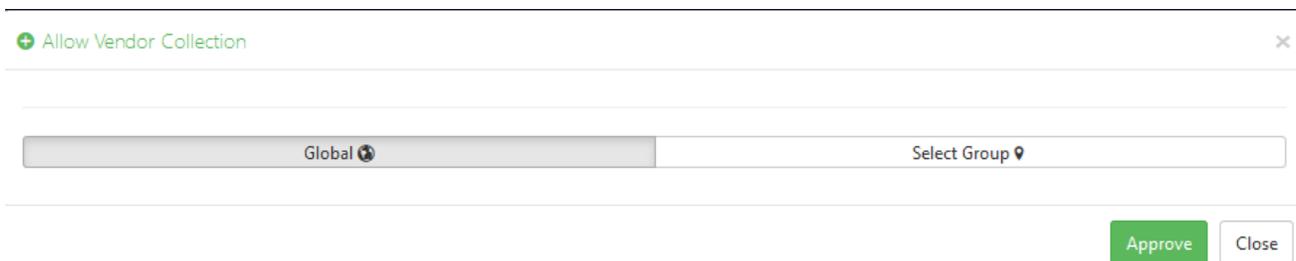


Figure 55

2. If you select Global and click **Approve**, it will enable the vendors in all the groups.
3. If you select **Selected Group** and click **Approve**, it will enable the vendors only from selected groups.

You can select the selected Groups from the Available Groups list.

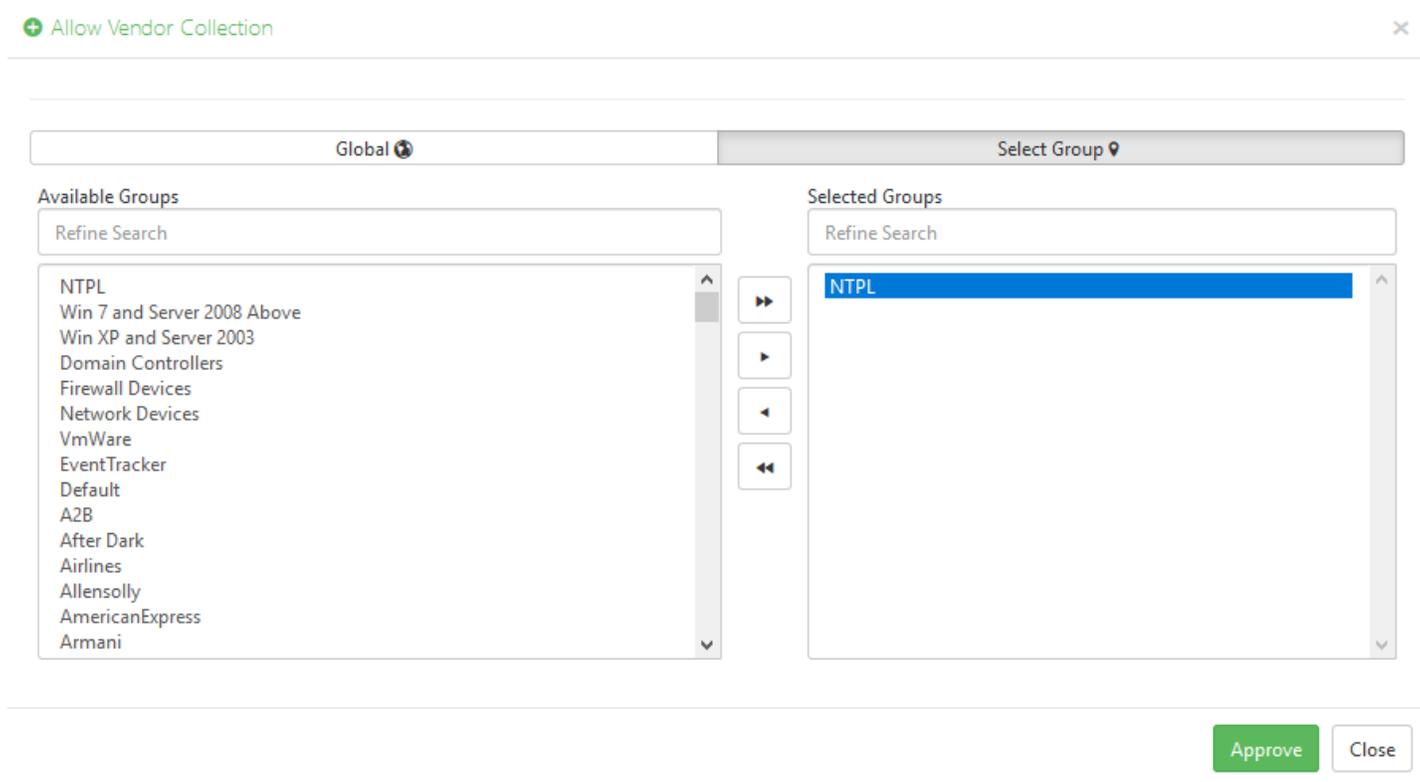


Figure 56

- The approved vendor group is seen in the **APPROVED VENDOR GROUPS** tab.

Processes

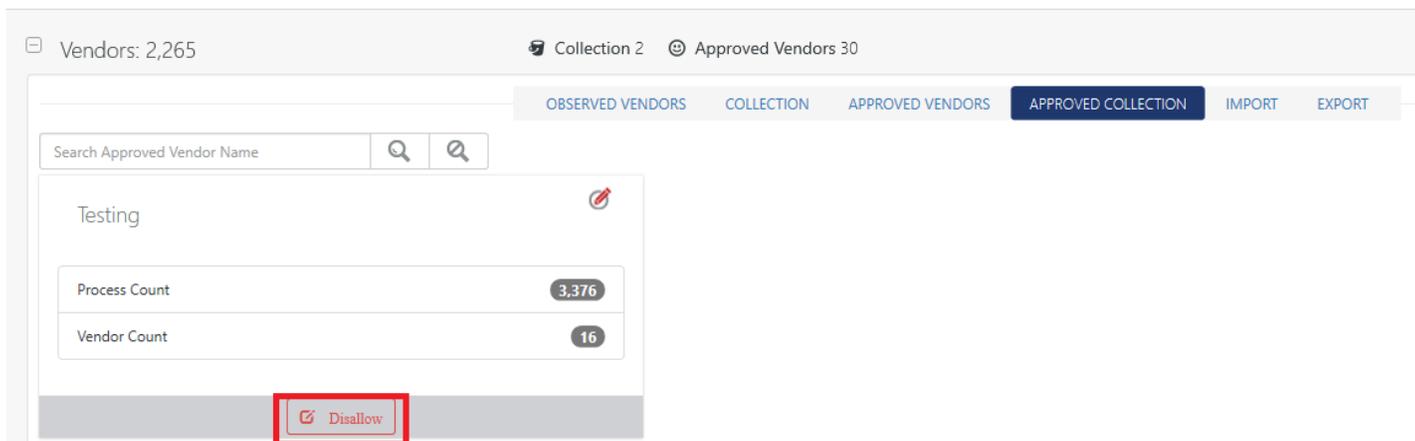


Figure 57

- You can click **Disallow** to disallow the vendor.

### 7.1.5 Import Vendors

- The user can click the **Import Vendors option** to import vendors based on **Signer** or **Product**.



Figure 58

### 7.1.6 Export Vendors

- You can click the **Export Vendors option**, to Export Vendors based on **Signer** or **Product**.

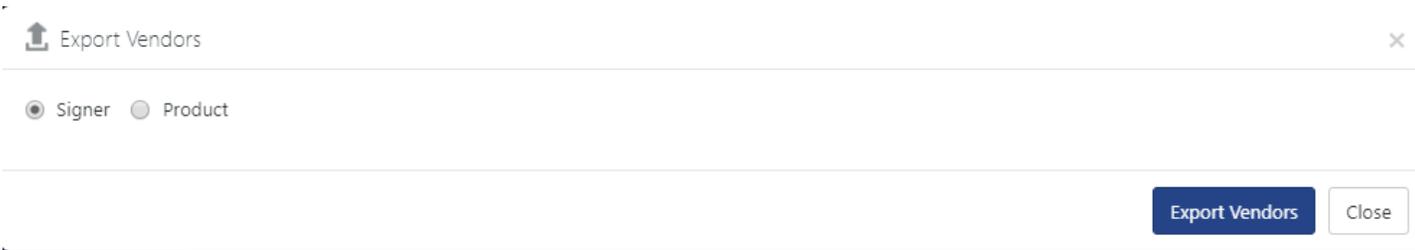


Figure 59

## 7.2 Rules

1. Click  icon to expand the Rules tab.

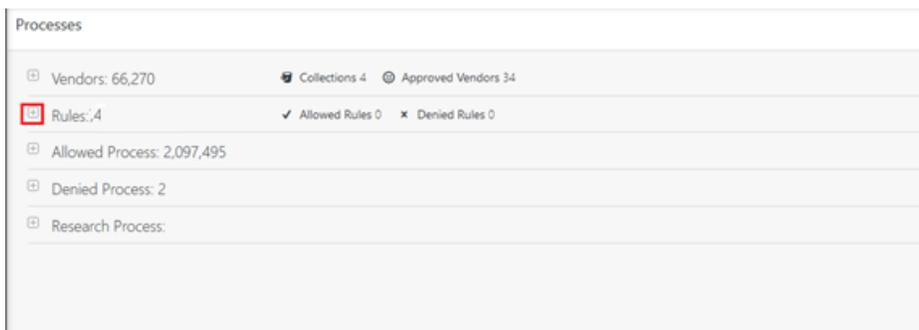


Figure 60

Rules are used to approve or deny any processes that are running in any given path.



Figure 61

2. To allow the rules, click the **ALLOWED RULES** tab, choose the **New Allowed Rule** tab.

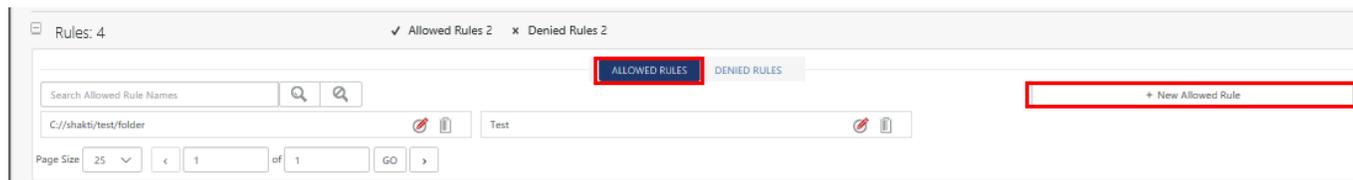


Figure 62

3. In the **Add Rule** window, type in the path or navigate to the process location and click **Add** to allow the rule. You may also check the option **“Allow Child process”** to allow the child processes.

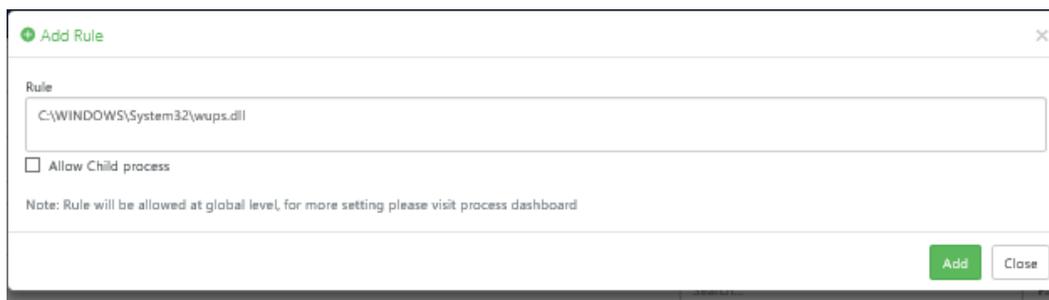


Figure 63

- Similarly, to deny the rules click the **DENIED RULES** tab and choose the **New Denied Rule** tab.

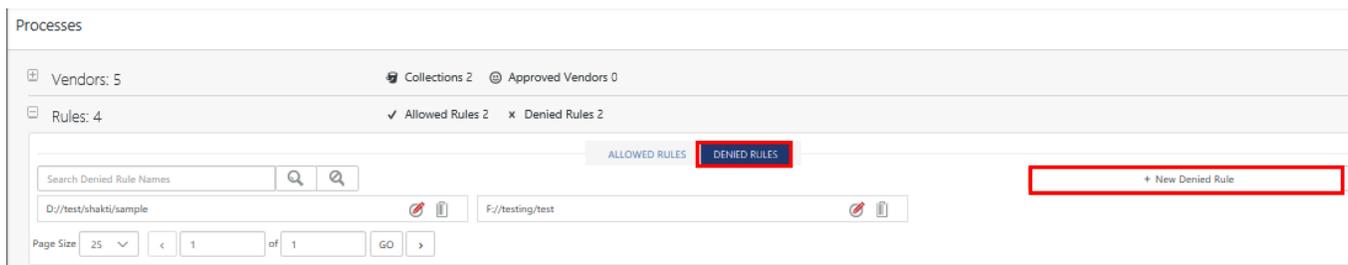


Figure 64

- In the **Add Rule** window, type in the path or navigate to the process location and click **Add** to deny the rule. You may also check the option **Allow Child process** to allow the child processes.

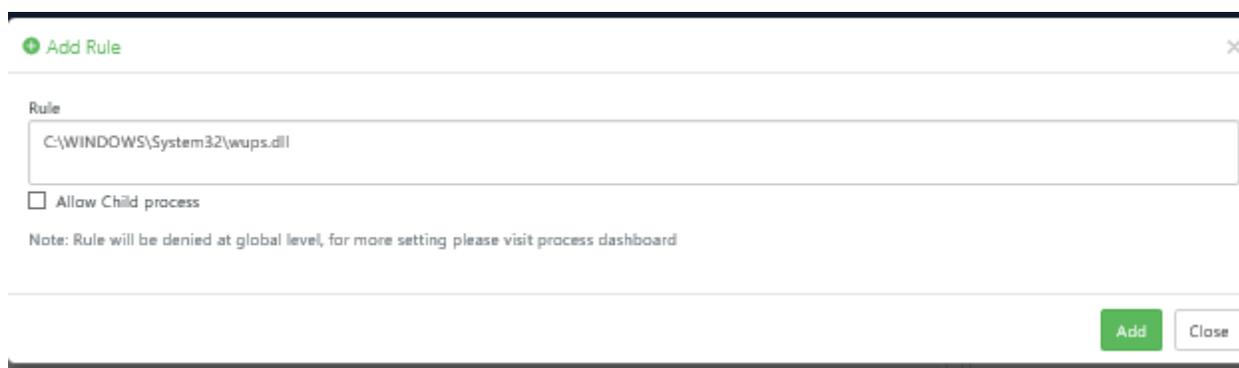


Figure 65

## 7.3 Allowed Process

- Click the **Expand**  icon next to the Allowed Process.

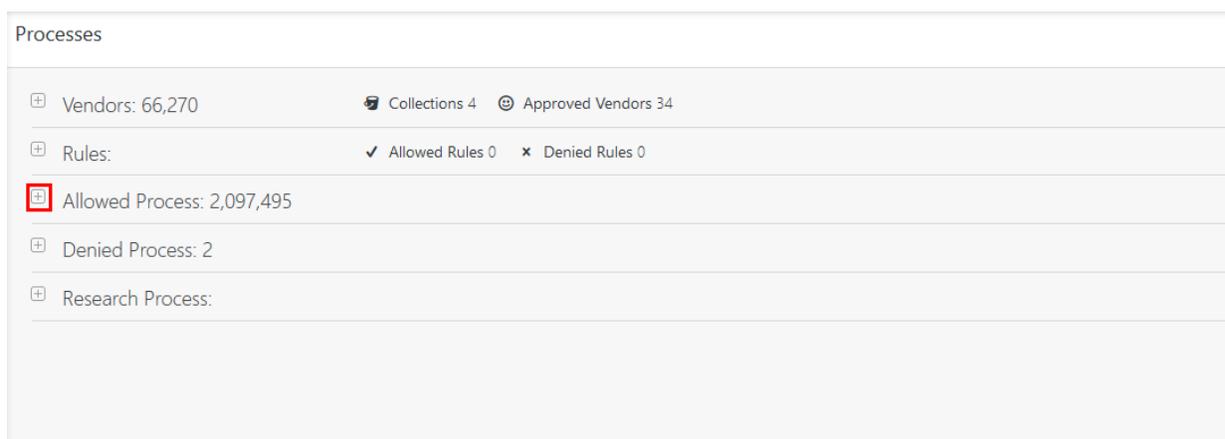


Figure 66

- Allowed Process appears where the user can view the processes that are allowed.

Allowed Process: 2,097,459

Search 'Hash' or 'File'

File Name	Opinion	Places
<input type="checkbox"/> wuaueng.dll	UNKNOWN	2
<input type="checkbox"/> appraiser.dll	UNKNOWN	2
<input type="checkbox"/> microsoft.sqlserver.configuration.rsexension.resources.dll	SAFE	0
<input type="checkbox"/> microsoft.sqlserver.configuration.resources.dll	SAFE	0
<input type="checkbox"/> microsoft.sqlserver.configuration.repl_configextension.resources.dll	SAFE	0

Figure 67

3. Click the **Expand**  icon next to the individual file name

Allowed Process: 2,097,459

Search 'Hash' or 'File'

File Name	Opinion	Places
<input checked="" type="checkbox"/> wuaueng.dll	UNKNOWN	2
<input type="checkbox"/> appraiser.dll	UNKNOWN	2
<input type="checkbox"/> microsoft.sqlserver.configuration.rsexension.resources.dll	SAFE	0
<input type="checkbox"/> microsoft.sqlserver.configuration.resources.dll	SAFE	0
<input type="checkbox"/> microsoft.sqlserver.configuration.repl_configextension.resources.dll	SAFE	0

Figure 68

Here, you can get an insight into the Allowed process that is chosen. Information like **FILE PATH, FILE MODIFIED TIME, SIGNED BY, COUNTER SIGNED BY, File names found, Detected on sensors, Actions Taken** is found.

Allowed Process: 2,097,459

Search 'Hash' or 'File'

File Name	Opinion	Places
wuaueng.dll	UNKNOWN	2

File Name  
wuaueng.dll

File Version: 10.0.17134.1

Product Name: Microsoft® Windows® Operating System

Signed By: N/A

Counter Signed By: N/A

Signed On:

File Modified Time: Jul 18 09:16:39 AM

File Path: C:\Windows\System32\wuaueng.dll

---

MD5 Checksum: 1dea4d396ed7c1c895e5cd13f60ed10d

Hash Opinion: UNKNOWN

Opinion Reference:

VirusTotal Ratio: 0/0

VirusTotal Link: [www.virustotal.com](http://www.virustotal.com)

Threat Engine: [IBM XFE](#) [Malc0de](#) [Team Cymru](#)

File names found: 1

wuaueng.dll

Figure 69

4. The user can click on the **Setting** icon, to **Allow** or **Deny** the process from the Allowed processes.

Allowed Process: 2,097,459

Search 'Hash' or 'File'

File Name	Opinion	
wuaueng.dll	UNKNOWN	<input type="button" value="✓ Allow"/> <input type="button" value="✗ Deny"/> <input type="button" value="⋮"/>

File Name  
wuaueng.dll

File Version: 10.0.17134.1

Product Name: Microsoft® Windows® Operating System

Signed By: N/A

Counter Signed By: N/A

Signed On:

File Modified Time: Jul 18 09:16:39 AM

File Path: C:\Windows\System32\wuaueng.dll

---

MD5 Checksum: 1dea4d396ed7c1c895e5cd13f60ed10d

Hash Opinion: UNKNOWN

Opinion Reference:

VirusTotal Ratio: 0/0

VirusTotal Link: [www.virustotal.com](http://www.virustotal.com)

Threat Engine: [IBM XFE](#) [Malc0de](#) [Team Cymru](#)

File names found: 1

wuaueng.dll

Figure 70

## 7.4 Denied Process

1. Click the Expand  icon next to the **Denied Process**.

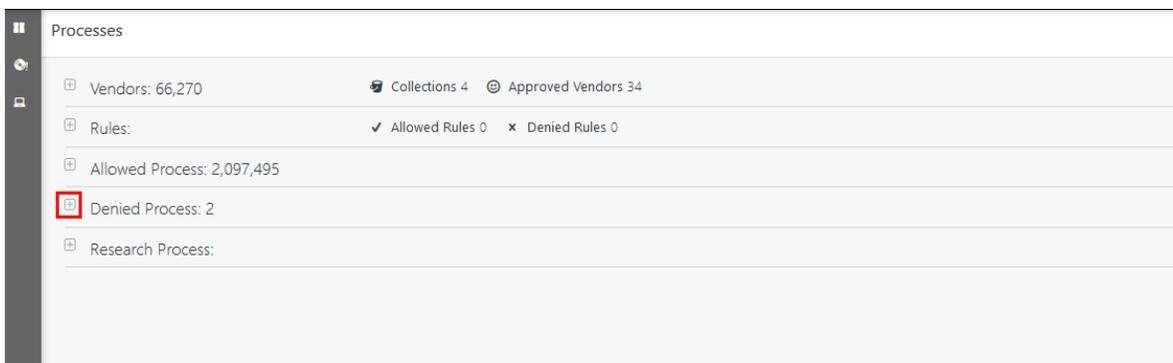


Figure 71

2. Denied Process appears, where you can view the processes that are denied.

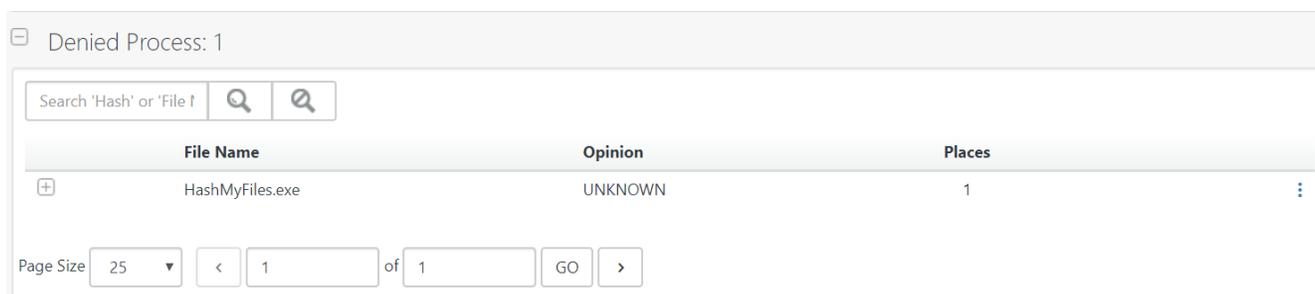


Figure 72

3. Click the **Expand**  icon next to the individual file name.



Figure 73

Information about **FILE PATH, FILE MODIFIED TIME, SIGNED BY, COUNTER SIGNED BY, File names found, Detected on sensors, Actions Taken** is found when the denied process is chosen.

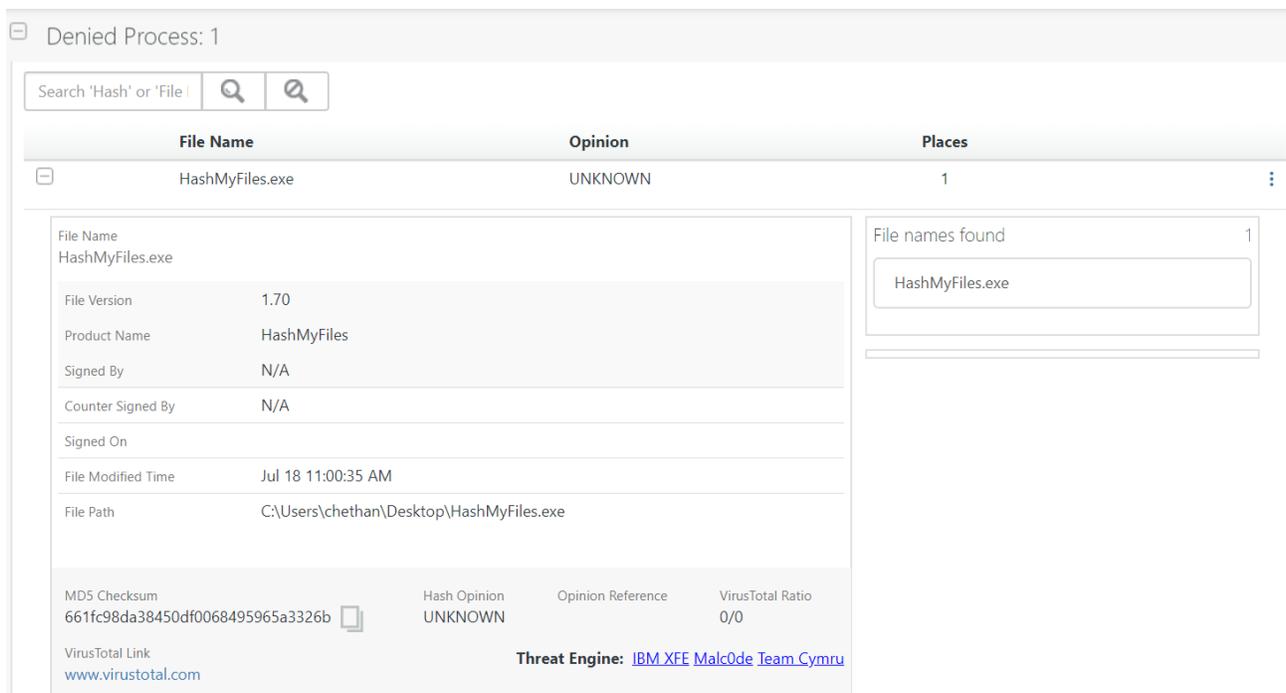


Figure 74

4. The user can click on the **Setting** icon, to **Allow** or **Deny** the process from the Denied processes.

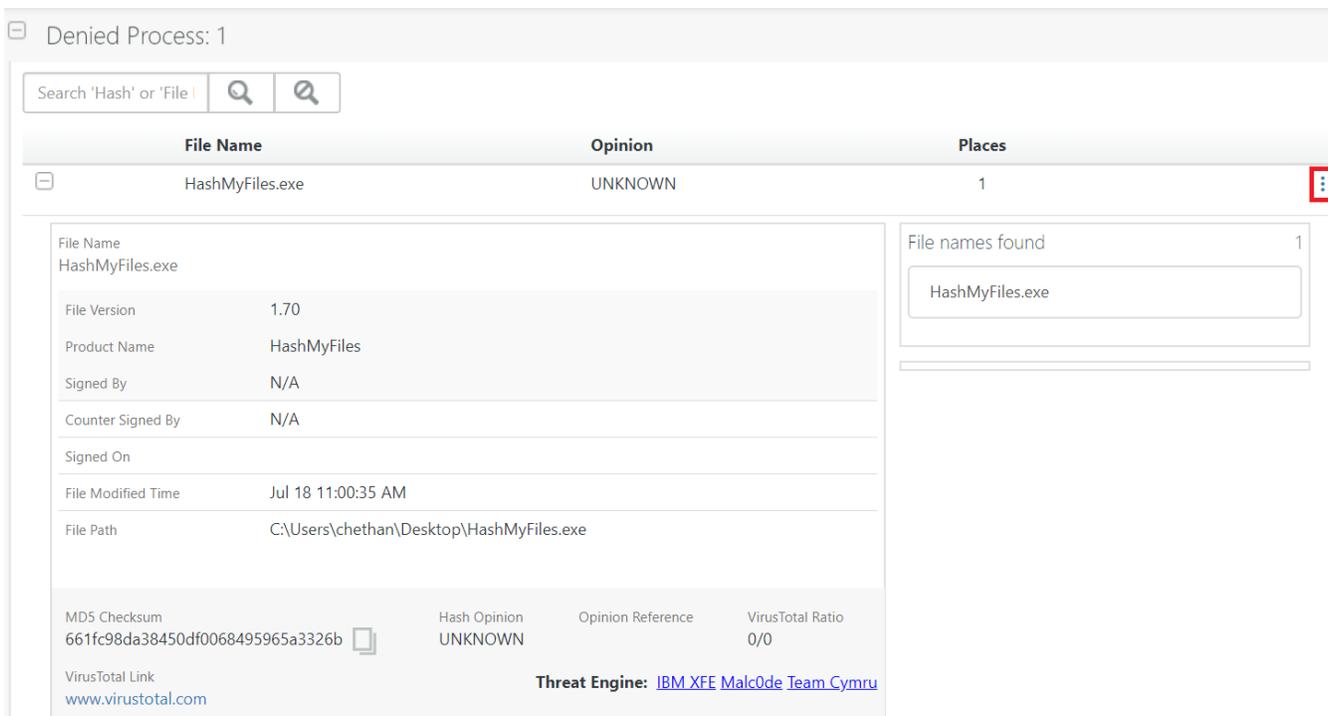


Figure 75

## 7.5 Research Process

1. Click the **Expand**  icon next to the Research Process

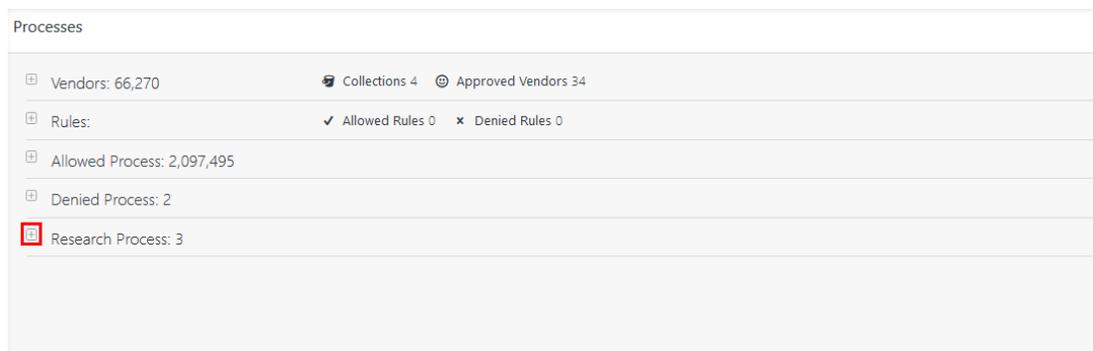


Figure 76

2. The **Research** Process appears, where you can view the processes that are been researched.

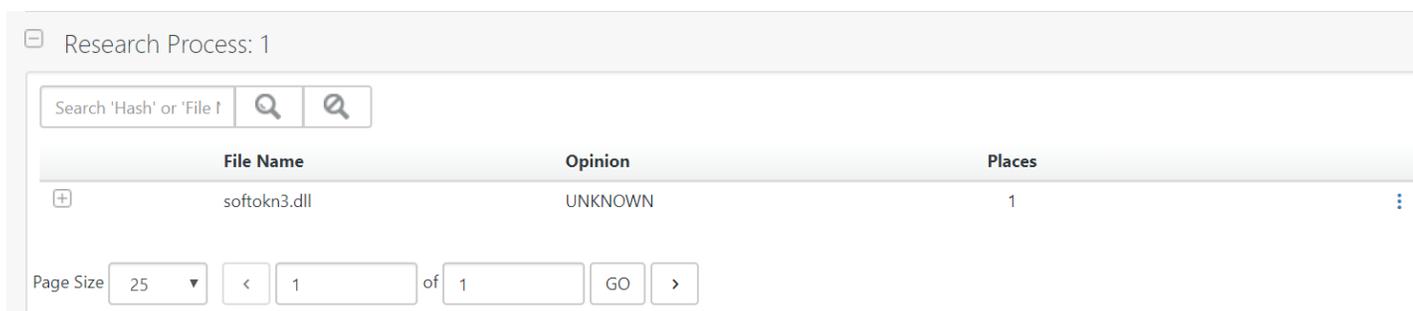


Figure 77

3. Click the **Expand**  icon next to the individual file name

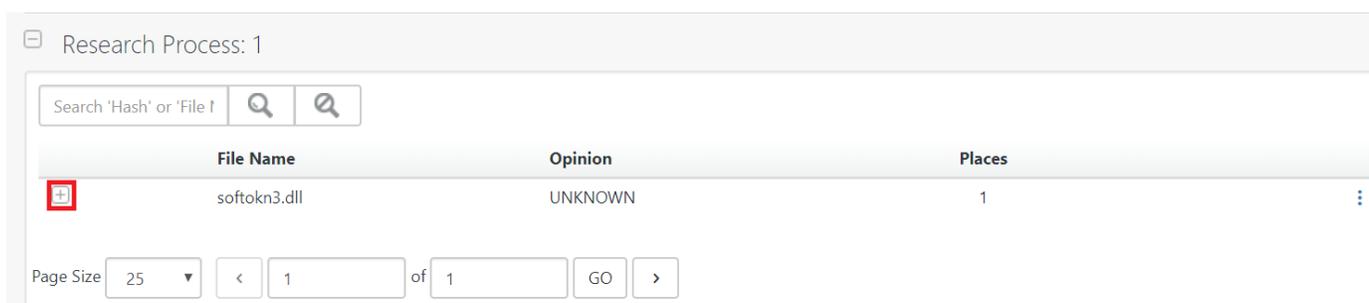


Figure 78

**FILE PATH, FILE MODIFIED TIME, SIGNED BY, COUNTER SIGNED BY, File names found, Detected on sensors, Actions Taken** is found, by expanding the Researched individual file name.

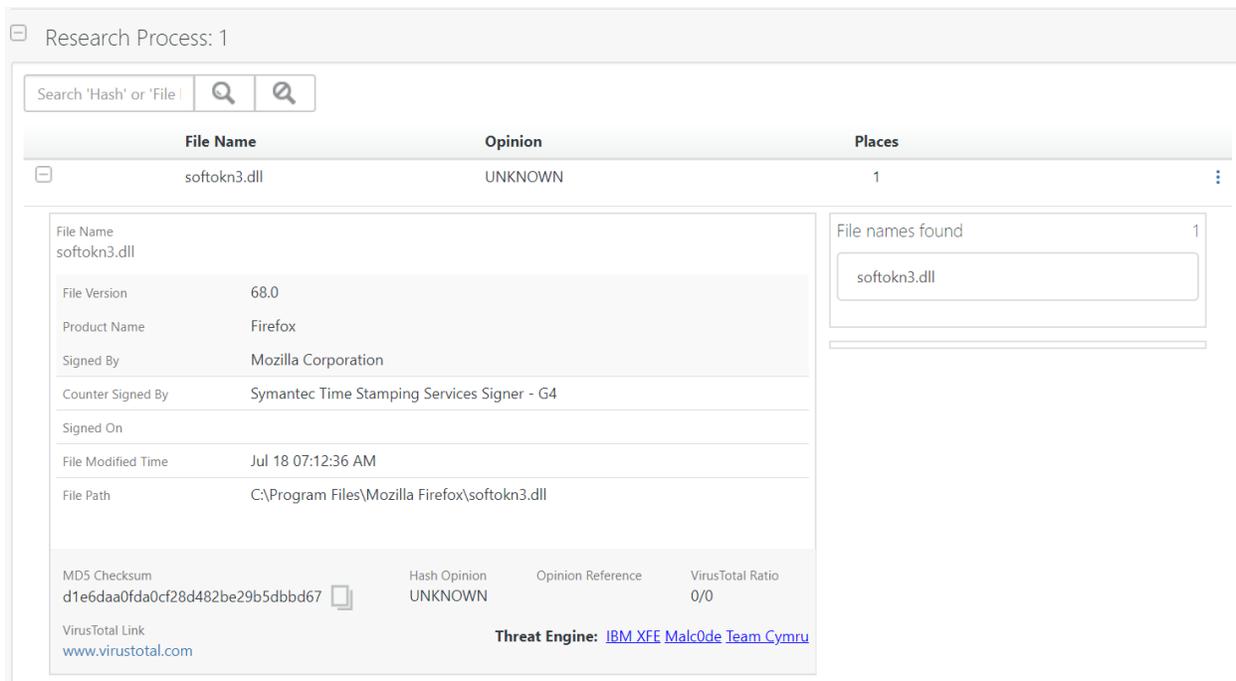


Figure 79

4. The user can click on the **Setting** icon, to **Allow** or **Deny** the process from the Denied processes.

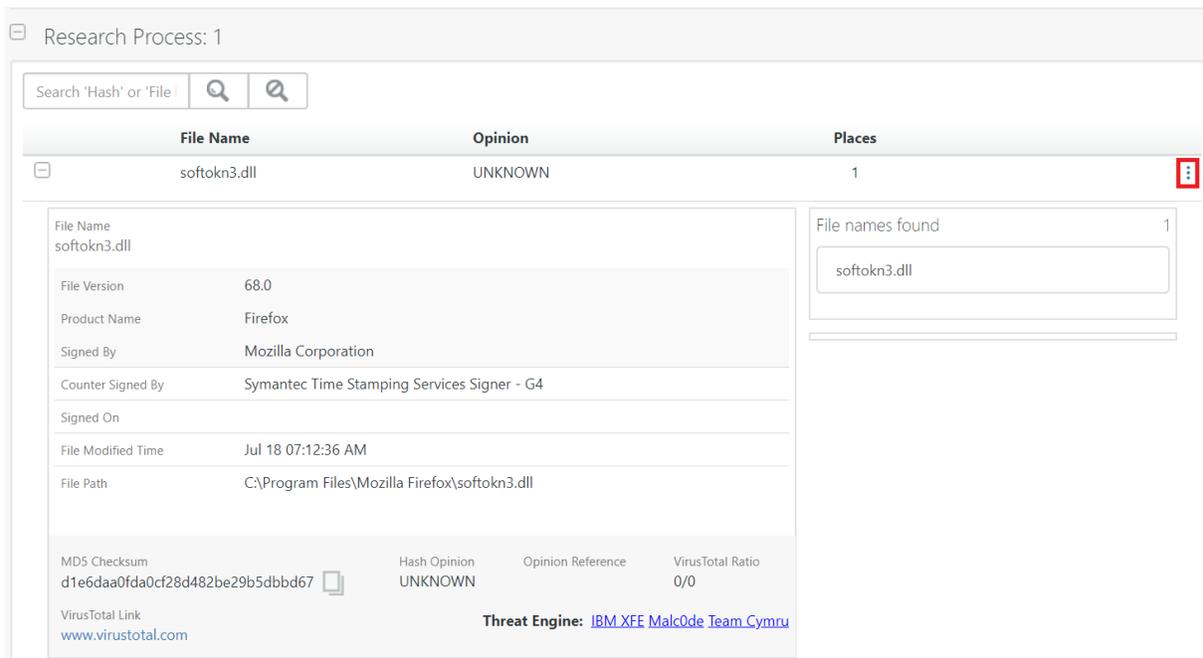


Figure 80

## 8. Sensors page

1. On the left Ribbon, click **Sensor**  to navigate to the sensor page.
2. The page contains information like the overview of the sensors in the dashboard.

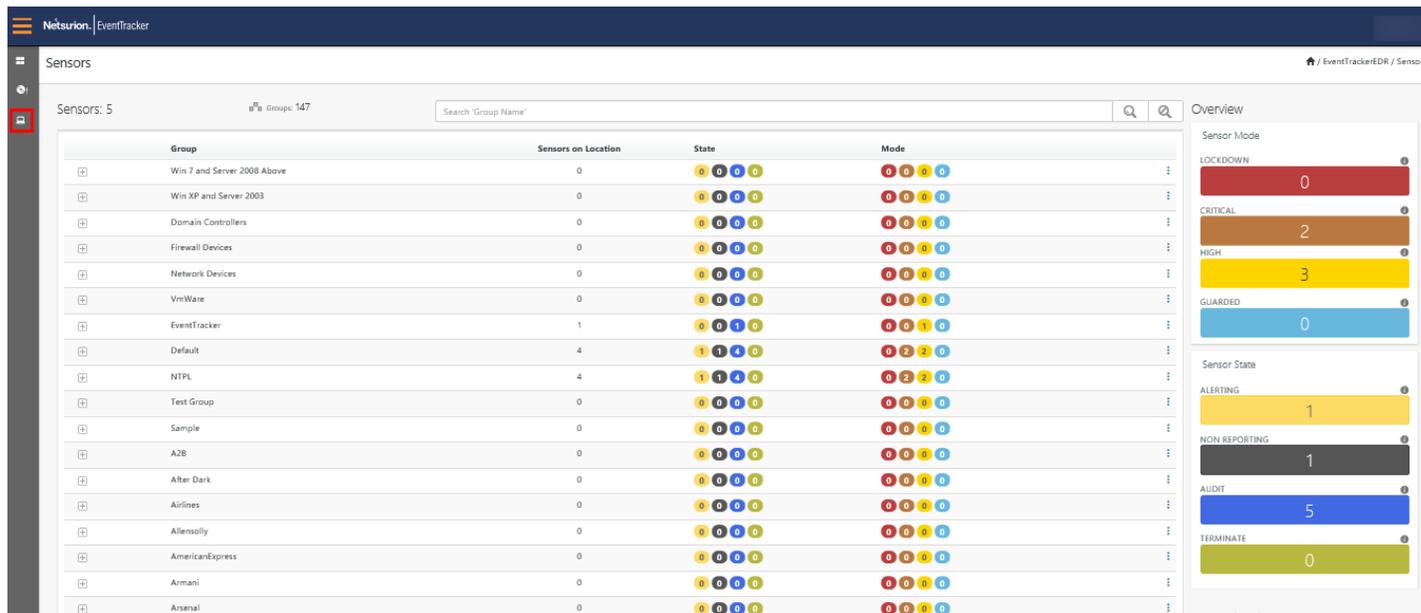


Figure 81

Each color represents the sensor’s Mode and the sensor’s State.

Color	Mode
Red	Lockdown
Orange	Critical
Yellow	High
Blue	Guarded

Color	State
Yellow	Alerting
Black	Non-Reporting
Blue	Audit
Teal	Terminate

3. The color and count imply the state and the mode of the process and their respective count.

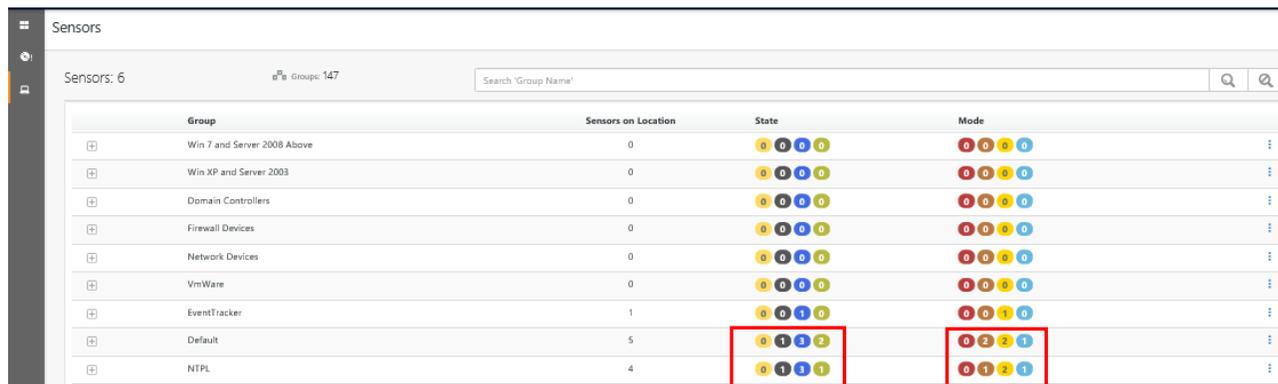


Figure 82

4. Click the tools option  , to change the **Group Mode** and the action.

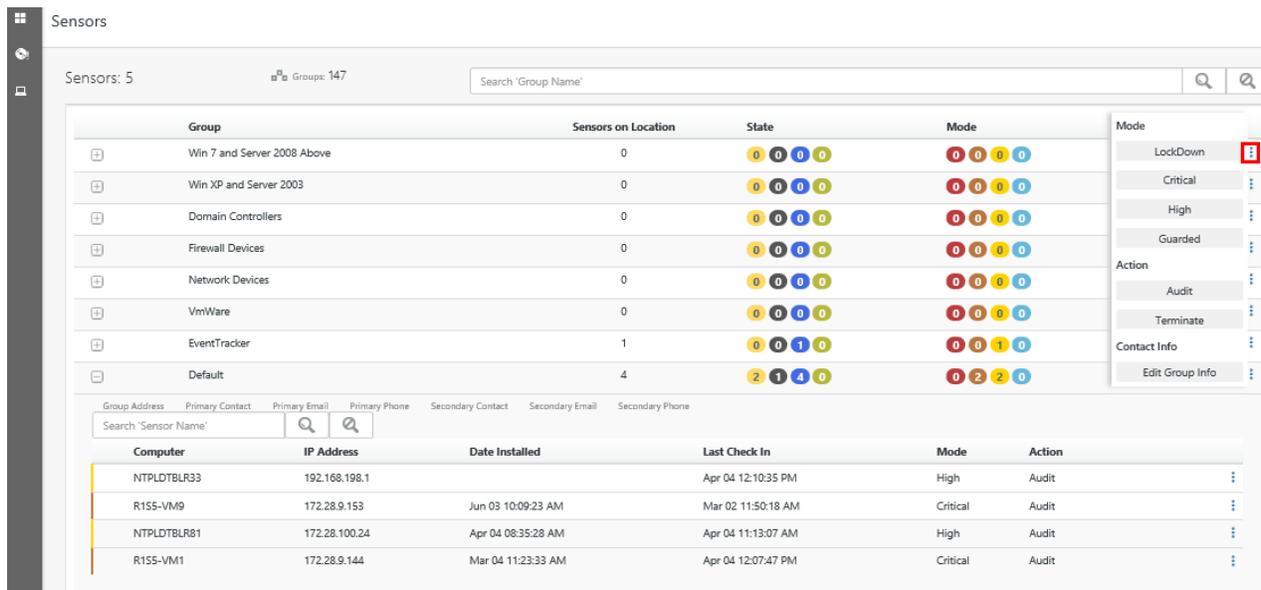


Figure 83

## 8.1 Edit Group Info

**Edit Group Info** option is used to edit the group information.

Click **Edit Group Info** to open the **Edit Group** window.

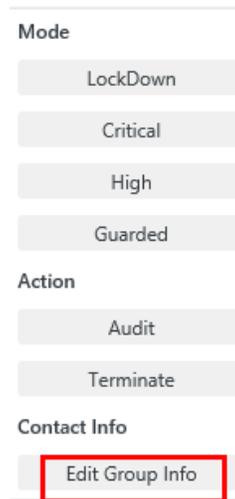


Figure 84

Once the required information is filled, click **Update Group** to update the Group Identification.

Edit Group ×

GROUP IDENTIFICATION

Group Name

Win 7 and Server 2008 Above

LOCATION / ADDRESS

Address1

Address2

City

Zip

State

Country

CONTACT INFO

Primary Contact Name

Secondary Contact Name

Primary Contact

Secondary Contact

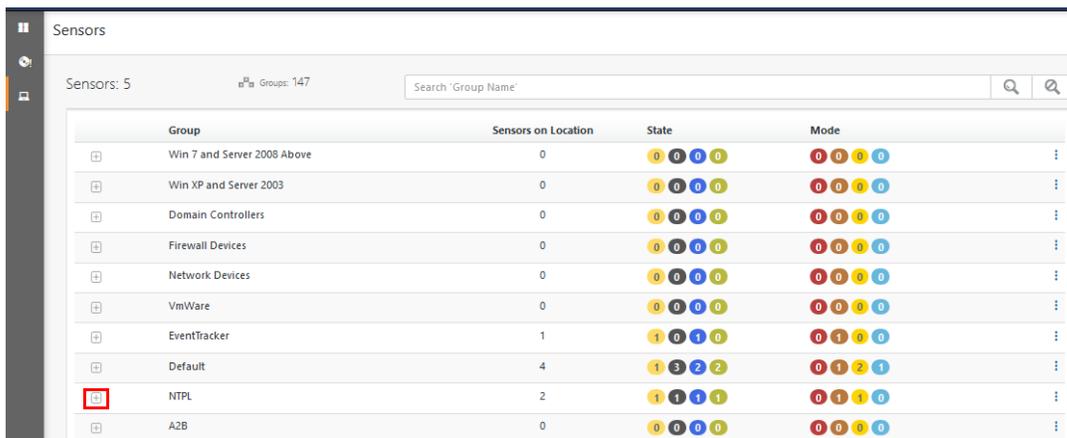
Primary Email

Secondary Email

Close Update Group

Figure 85

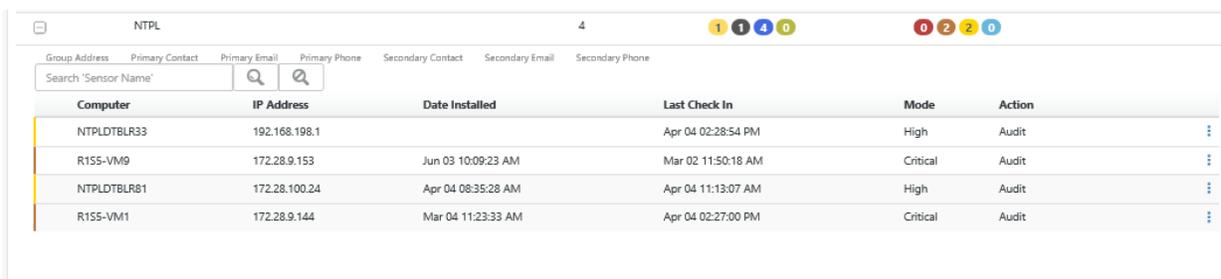
1. Click **Expand**  icon next to the **Group**, to access more information about the selected group.



Group	Sensors on Location	State	Mode
Win 7 and Server 2008 Above	0	0 0 0 0	0 0 0 0
Win XP and Server 2003	0	0 0 0 0	0 0 0 0
Domain Controllers	0	0 0 0 0	0 0 0 0
Firewall Devices	0	0 0 0 0	0 0 0 0
Network Devices	0	0 0 0 0	0 0 0 0
VmWare	0	0 0 0 0	0 0 0 0
EventTracker	1	1 0 1 0	0 1 0 0
Default	4	1 3 2 2	0 1 2 1
<b>NTPL</b>	2	1 1 1 1	0 1 1 0
A2B	0	0 0 0 0	0 0 0 0

Figure 86

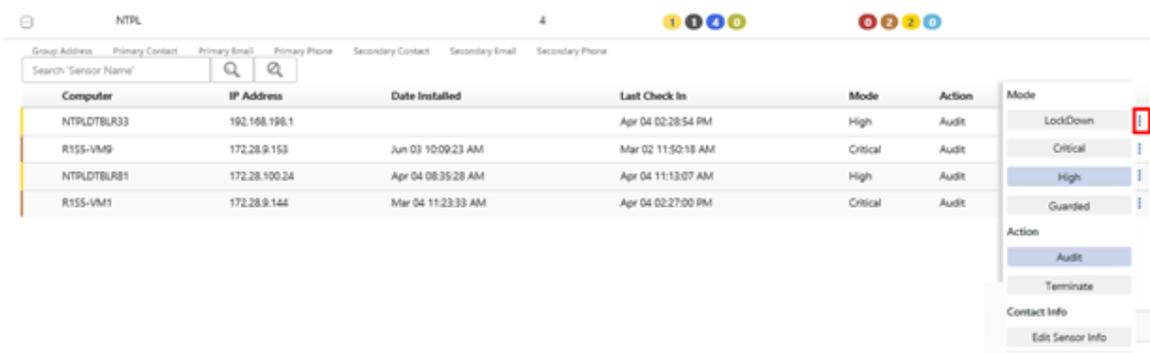
2. The selected group expands to provide information on the individual system present in the group. Here you can see information about the **Computer**, **IP Address**, **Date Installed**, **Last Check in**, **Mode**, and **Action**.



Computer	IP Address	Date Installed	Last Check In	Mode	Action
NTPLDTBLR33	192.168.198.1		Apr 04 02:28:54 PM	High	Audit
R155-VM9	172.28.9.153	Jun 03 10:09:23 AM	Mar 02 11:50:18 AM	Critical	Audit
NTPLDTBLR81	172.28.100.24	Apr 04 08:35:28 AM	Apr 04 11:13:07 AM	High	Audit
R155-VM1	172.28.9.144	Mar 04 11:23:33 AM	Apr 04 02:27:00 PM	Critical	Audit

Figure 87

3. The user can click **tools option**  , to change the Sensor **Mode** and **Action**.



Computer	IP Address	Date Installed	Last Check In	Mode	Action
NTPLDTBLR33	192.168.198.1		Apr 04 02:28:54 PM	High	Audit
R155-VM9	172.28.9.153	Jun 03 10:09:23 AM	Mar 02 11:50:18 AM	Critical	Audit
NTPLDTBLR81	172.28.100.24	Apr 04 08:35:28 AM	Apr 04 11:13:07 AM	High	Audit
R155-VM1	172.28.9.144	Mar 04 11:23:33 AM	Apr 04 02:27:00 PM	Critical	Audit

Figure 88

Change Sensor Mode

System Name  
NTPLDTBLR301

SENSOR MODE  
 Lockdown  Critical  High  Guarded

SENSOR ACTION  
 Audit  Terminate  
 Allow All Signed Process

Close Update Sensor Mode

Figure 89

## 8.2 Edit Sensor Info

**Edit Sensor Info** option is used to edit the sensor information.

1. Click **Edit Sensor Info** to open the **Edit Sensor** window.

Mode

LockDown

Critical

High

Guarded

Action

Audit

Terminate

Contact Info

Edit Sensor Info

Figure 90

2. Enter the information required and click **Update Sensor** to update the Sensor Identification.

**Edit Sensor** ×

---

**SENSOR IDENTIFICATION**

System Name

---

**LOCATION / ADDRESS**

Address1

Address2

City

Zip

Phone

Secondary Contact Name

Primary Contact

Secondary Contact

Primary Email

Secondary Email

---

Close Update Sensor

Figure 91

## 9. Agent Resource Utilization

EDR update on remote agent machine utilizes additional resources. This resource utilization varies depending on maintained safe and unsafe files.

**Agent CPU usage:** 15% to 20%.

**Agent Memory usage:** 430MB to 450MB.

**Note:** The above resource utilization will vary for other settings in the agent configuration. Example: Agent LFM.