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’s 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.

© 2020 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 Endpoint Detection and Response ............................................................................ 4
3. EDR vs Anti-virus .................................................................................................................. 4
4. Introducing Endpoint Detection and Response (EDR) in EventTracker v9.x ............................ 5
5. Accessing the Endpoint Detection and Response 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 .................................................................................. 17
   6.4.1 Bulk Action .................................................................................................................... 19
6.5 Action Taken Processes Pane ........................................................................................... 20
6.6 Overview of the Action Taken Processes ........................................................................... 22
7. Processes Page ....................................................................................................................... 22
   7.1 Vendors ........................................................................................................................... 23
   7.1.1 Observed Vendors tab ................................................................................................ 24
   7.1.2 Collection tab .............................................................................................................. 29
   7.1.3 Approved Vendors ....................................................................................................... 30
   7.1.4 Approved Collection .................................................................................................. 31
   7.1.5 Import .......................................................................................................................... 33
   7.1.6 Export ......................................................................................................................... 33
   7.2 Rules ............................................................................................................................... 34
   7.3 Allowed Process .............................................................................................................. 35
   7.4 Denied Process ................................................................................................................. 38
   7.5 Research Process ............................................................................................................. 40
8. Sensors .................................................................................................................................. 42
   8.1 Edit Group Info ............................................................................................................... 44
   8.2 Edit Sensor Info .............................................................................................................. 47
9. Agent Resource Utilization .................................................................................................... 49
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 Endpoint Detection and Response**

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.

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

4. Introducing Endpoint Detection and Response (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 Endpoint Detection and Response from EventTracker

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

   ![Figure 1](image1.png)

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

   ![Figure 2](image2.png)
EventTracker EDR Dashboard opens (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. You can change the Groups view to Map view by toggling Select View Type option.
- **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.
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.
• Each color indicates a Group status.

<table>
<thead>
<tr>
<th>Color</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yellow</td>
<td>ALERTING</td>
<td>This status shows all the locations or systems where a new process has appeared.</td>
</tr>
<tr>
<td>Gray</td>
<td>NON-REPORTING</td>
<td>This status shows that we have not received a ‘keep alive’ status from there systems or locations.</td>
</tr>
</tbody>
</table>

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

Figure 5

Figure 6

Figure 7
• The status and the description are shown in the following table.

<table>
<thead>
<tr>
<th>Color</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orange 0</td>
<td>DORMANT</td>
<td>Indicates the number of files detected before execution.</td>
</tr>
<tr>
<td>Red 0</td>
<td>TERMINATED</td>
<td>Indicates the Terminated process by the EventTracker EDR.</td>
</tr>
<tr>
<td>Fountain Blue</td>
<td>NOT TERMINATED</td>
<td>Indicates the process that ran during the maintenance mode and is now running without disposition.</td>
</tr>
</tbody>
</table>

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](image)

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](image)
### 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.

- **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](image)

- **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](image)
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 many 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.

- 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, with out 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.
Click [ ] to know more about the process details.

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

Allowing the process

1. Click Allow and it opens the Allow Process dialog box.
2. When **Global** option is selected, clicking **Allow**, selects all the groups in the environment.

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

---

**Denying the process**

1. Click **Deny**, to open the **Deny Process** dialog box.
Figure 19

2. 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.

![Deny Process](image)

Figure 20

- 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.

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**.
• The status and the description are shown in the following table.

<table>
<thead>
<tr>
<th>Color</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red 0</td>
<td>TERMINATED</td>
<td>Indicates the Terminated process by the EventTracker EDR.</td>
</tr>
<tr>
<td>Fountain Blue 0</td>
<td>NOT-TERMINATED</td>
<td>Indicates the process that ran during the maintenance mode and is now running without disposition.</td>
</tr>
<tr>
<td>Orange 0</td>
<td>DORMANT</td>
<td>Indicates the number of files detected before execution.</td>
</tr>
</tbody>
</table>

• **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.

![Figure 23](image)

• **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.

![Figure 24](image)
- **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 25](image-url)

**6.4.1 Bulk Action**

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 26](image-url)

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.
6.5 Action Taken Processes Pane

This pane displays the corrective actions (response) taken for events and incidents. You can see the overview of all the processes that are Allowed, Denied or Researched after the action is taken.

1. Click on the icon to expand the tab. You will see the detailed information about the File Names and the corrective action taken.
2. 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.
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.

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 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 35](image)

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

<table>
<thead>
<tr>
<th>Color</th>
<th>Processes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>ALLOWED</td>
<td>The number of processes that were Allowed.</td>
</tr>
<tr>
<td>Red</td>
<td>DENIED</td>
<td>The number of processes that were Denied.</td>
</tr>
<tr>
<td>Blue</td>
<td>RESEARCH</td>
<td>The number of processes that were Researched.</td>
</tr>
</tbody>
</table>

### 7.1 Vendors

Click 📚 icon on the vendor’s tab.
The Vendors page opens with the following tabs:

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

7.1.1 Observed Vendors tab

- It displays all the vendors present in the environment.
You can view or search vendors based on Signer or Product Vendors. When you select **Show Signer**, you can view only the Signer Vendors.

When you select **Show Product**, you can view only the Product Vendors.
When you select both the options, you can view both Signer and Product vendors.

Click “+ Create New Signer Collection” tab to create new vendors and edit vendor groups.
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.
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 44

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

Figure 45

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

![Add Vendor Collection](image)

**Figure 46**

### 7.1.2 Collection tab

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

![Collection tab](image)

**Figure 47**

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.

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.
7.1.4 Approved Collection

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

![Figure 50]

- 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 51]

1. Click the icon present on the respective vendors to open the “**Allow Vendor Collection**” dialog box.
2. If you select Global and click Approve, it will enable the vendors in all the groups.
3. If you select Select Group and click Approve, it will enable the vendors only from selected groups.

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

4. The approved vendor group is seen in the APPROVED VENDOR GROUPS tab.
5. You can click **Disallow** to disallow the vendor.

### 7.1.5 Import

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

![Image](image_url)

**Figure 55**

### 7.1.6 Export

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

![Image](image_url)

**Figure 56**
7.2 Rules

1. Click icon to expand the Rules tab.

![Figure 57]

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

![Figure 58]

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

![Figure 59]

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 60]
4. Similarly, to deny the rules click the **DENIED RULES** tab and choose the **New Denied Rule** tab.

![Figure 61](image.png)

5. 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 62](image.png)

7.3 **Allowed Process**

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

![Figure 63](image.png)

2. **Allowed Process** appears where the user can view the processes that are allowed.
3. Click the Expand icon next to the individual file name

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

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

![Figure 68](image1)

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

![Figure 69](image2)

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

![Figure 70](image3)

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

1. Click the Expand icon next to the Research Process

![Figure 73](image)

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

![Figure 74](image)

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

![Figure 75](image)

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

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.

![Sensors page screenshot]

*Figure 78*

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

<table>
<thead>
<tr>
<th>Color</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>Lockdown</td>
</tr>
<tr>
<td>Orange</td>
<td>Critical</td>
</tr>
<tr>
<td>Yellow</td>
<td>High</td>
</tr>
<tr>
<td>Blue</td>
<td>Guarded</td>
</tr>
</tbody>
</table>
3. The color and count imply the state and the mode of the process and their respective count.

<table>
<thead>
<tr>
<th>Color</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yellow</td>
<td>Alerting</td>
</tr>
<tr>
<td>Black</td>
<td>Non-Reporting</td>
</tr>
<tr>
<td>Blue</td>
<td>Audit</td>
</tr>
<tr>
<td>Teal</td>
<td>Terminate</td>
</tr>
</tbody>
</table>

![Figure 79](image1)

4. Click the tools option ![Tools](image2), to change the **Group Mode** and the action.

![Figure 80](image3)
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 81](image)

Once the required information is filled, click *Update Group* to update the Group Identification.
Figure 82
1. Click Expand icon next to the Group, to access more information about the selected group.

![Figure 83](image)

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.

![Figure 84](image)

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

![Figure 85](image)
8.2 Edit Sensor Info

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

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

2. Enter the information required and click **Update Sensor** to update the Sensor Identification.
Figure 88
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.