



User Guide

The Netsurion Open XDR platform's Application Control Dashboard

Publication Date:

March 30, 2023

Abstract

This document gives a brief overview of the Netsurion Open XDR platform Application Control Dashboard's User Interface, which is an integrated security solution providing an additional layer of surveillance and visibility for your enterprise across your IT network.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Audience

This guide is intended for all the Netsurion Open XDR platform users responsible for managing network security, and the users of the Netsurion Open XDR platform version 9.x who intend to learn the Application Control Dashboard.

This guide assumes that you are well-informed of your entire enterprise networking.

Note:

This guide is updated for Open XDR version v9.4 and some functionality may not exist in Open XDR version 9.3.

Product Terminology

The following are the terms used throughout this guide:

- The term "Netsurion's Open XDR platform" or "the Netsurion Open XDR platform" or "the Open XDR platform" refers to EventTracker.

Table of Contents

- 1 Overview.....4**
- 1.1 Uses of Application Control 4
- 1.2 Application Control vs Anti-Virus..... 4
- 2 Application Control in the Netsurion Open XDR platform v9.x..... 5**
- 2.1 What’s New in version 9.4? 5
- 2.2 Accessing the Application Control 6
- 3 Application Control Dashboard 8**
- 3.1 Groups Pane 11
- 3.1.1 Groups Overview 12
- 3.2 Pending Analyst Pane 13
- 3.2.1 Pending Analyst Overview 24
- 3.3 Action Taken Processes Pane..... 26
- 3.3.1 Action Taken Processes Overview 27

1 Overview

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 the Open XDR platform's Application Control. Application Control tool is an adaptive, superior, and thorough technology for protecting the endpoints in your network. Application Control Solutions are exclusively designed for monitoring and responding to the Advanced Internet Threats.

Application Controls are installed as agents or sensors for the endpoints, from where security data are collected and sent to a centralized location for further analysis. Application Control solutions help in analyzing and identifying the patterns and detecting malware, which can be notified as alerts for remedial actions or any investigation.

Features

The Netsurion Open XDR platform's Application Control capabilities mainly include:

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

1.1 Uses of Application Control

To safeguard the network or endpoints in your network, you must use the Application Control tool as an advanced security solution.

You should install Application Control 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.

1.2 Application Control vs Anti-Virus

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

An Application Control security solution is centrally managed and remotely controlled security operations. Application Control 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 the endpoint protection platform. Antivirus covers a single endpoint and only detects and blocks malicious files.

Application Control vs Anti-Virus

Application Control	Antivirus
<ul style="list-style-type: none"> ▪ Protects complete network and all its endpoints. Security solution for the entire organization. 	<ul style="list-style-type: none"> ▪ Protects individual devices: Security solution for each workstation.
<ul style="list-style-type: none"> ▪ Threat identification and protection: Includes endpoint protection capabilities such as anti-malware, firewalls. 	<ul style="list-style-type: none"> ▪ Threat identification: Detects different types of malwares including viruses.
<ul style="list-style-type: none"> ▪ Dashboards, reports, and alert warnings to help continuous monitoring. 	<ul style="list-style-type: none"> ▪ Alerts
<ul style="list-style-type: none"> ▪ Incident investigations and Response. 	<ul style="list-style-type: none"> ▪ Scheduled scans
<ul style="list-style-type: none"> ▪ Identifies and blocks lateral movement across networks. ▪ Provides post-breach visibility. 	

2 Application Control in the Netsurion Open XDR platform v9.x

The Netsurion Open XDR platform v9.x has integrated Application Control interface that works in strengthening your network security. Application Control was introduced in the Open XDR platform 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, Application Control was introduced.

Application Control includes the following services:

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

2.1 What’s New in version 9.4?

From the Netsurion Open XDR platform Release 9.4 onwards, whenever a new process is detected the Hash lookup will first take place in the Netsurion Threat Center.

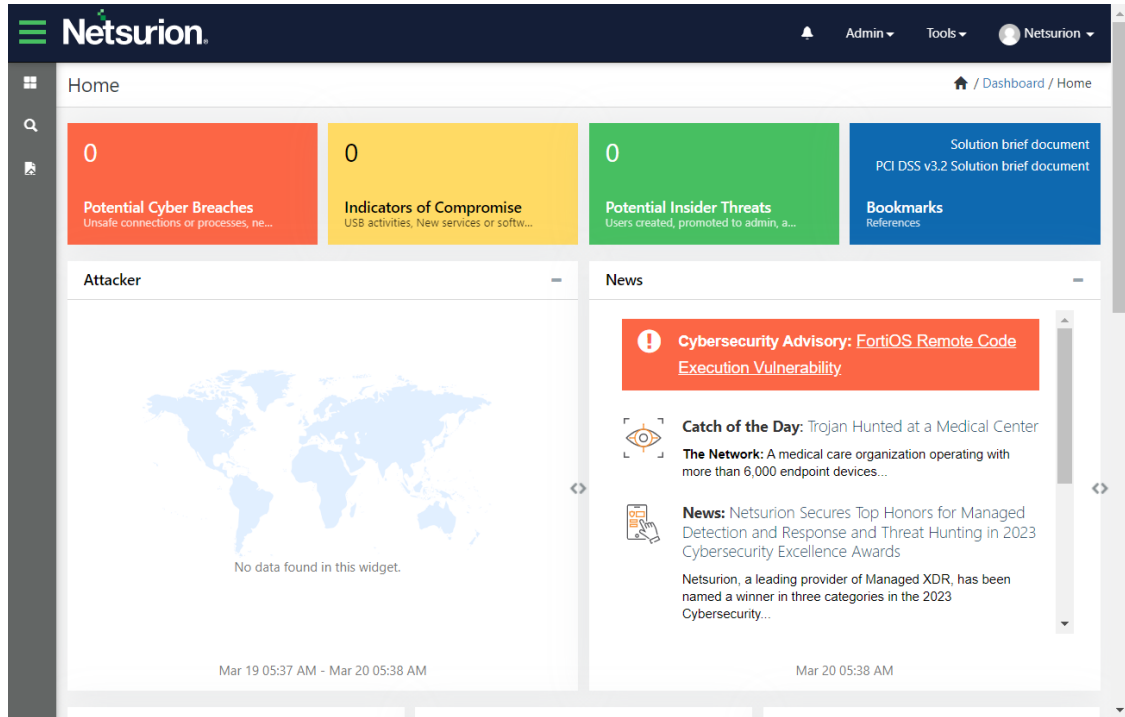
IMPORTANT:

If the Hash is not found in the Netsurion Threat Center or the lookup is not possible due to other circumstances, then the Hash will be looked up in the Virus Total.

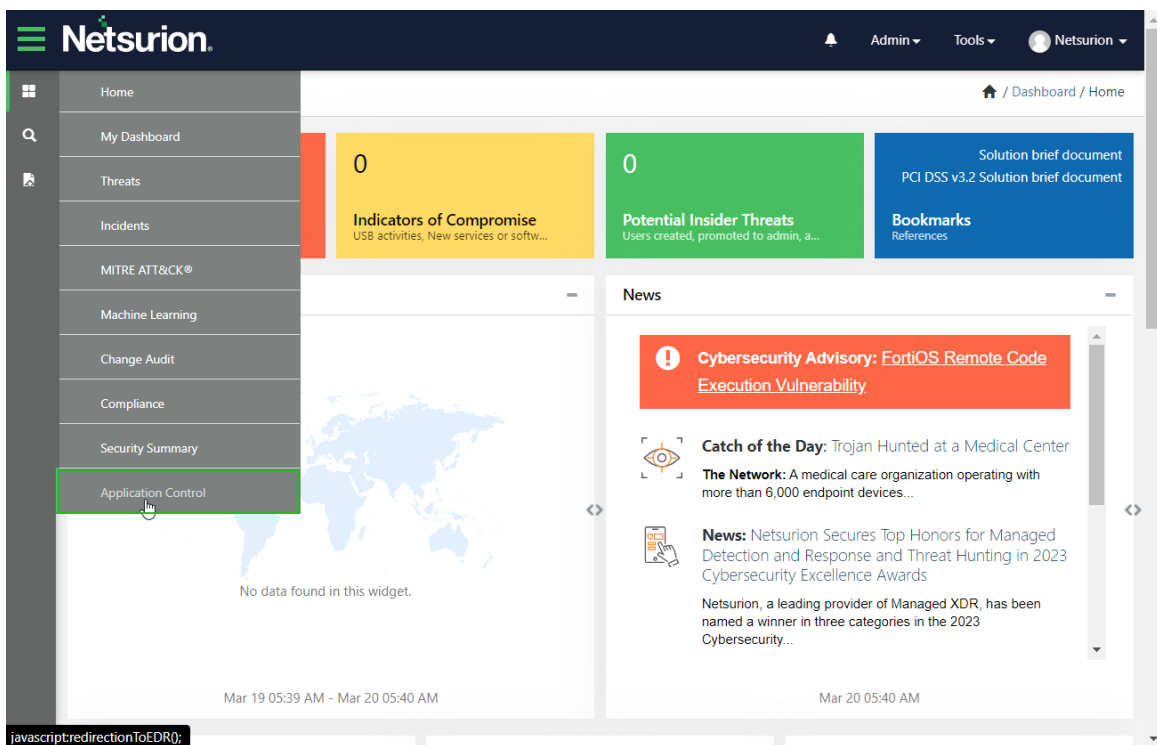
2.2 Accessing the Application Control

Perform the following process to go to the Application Control in the Netsurion Open XDR platform.

1. Log in to the Open XDR platform with the username and password.



2. In the left of the **Home** interface, hover over the **Dashboard** icon and click **Application Control** from the drop-down menu.



3. The Open XDR console navigates to the Application Control Dashboard.

Dashboard EventTracker / Application Control / Dashboard

Total Sensors: 4

Groups

Group	Total
Microsoft	1 Total
Apple	1 Total
Microsoft	1 Total
Microsoft	1 Total
Google	1 Total
Microsoft	1 Total
Default	0 Total
Microsoft	0 Total

Page Size: 25 of 1 GO

Overview

Sensors

ALERTING **4**

NON REPORTING **0**

Pending Analyst Review: 143

File Found Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places
0 minutes ago	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
0 minutes ago	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
0 minutes ago	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
2 minutes ago	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
2 minutes ago	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
2 minutes ago	System.dll	Microsoft	Microsoft	Low	SAFE	1
2 minutes ago	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
2 minutes ago	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
4 minutes ago	System.dll	Microsoft	Microsoft	Low	UNKNOWN	2
6 minutes ago	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
6 minutes ago	System.dll	Microsoft	Microsoft	Low	SAFE	1
6 minutes ago	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
6 minutes ago	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
6 minutes ago	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
6 minutes ago	System.dll	Microsoft	Microsoft	Low	SAFE	2
6 minutes ago	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
8 minutes ago	System.dll	Microsoft	Microsoft	Low	UNKNOWN	2
8 minutes ago	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
10 minutes ago	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
10 minutes ago	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
10 minutes ago	System.dll	Microsoft	Microsoft	Low	SAFE	1
10 minutes ago	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
10 minutes ago	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
12 minutes ago	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1

Page Size: 25 of 6 GO

Overview

143 Pending Processes

TERMINATED **0**

NOT TERMINATED **143**

DORMANT **0**

BULK ACTION

Allow All

Deny All

Action Taken Processes: 1,147

Action Taken Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places
6 minutes ago	System.dll	Microsoft	Microsoft	Low	SAFE	2
Aug 30 05:28:21 PM	System.dll	Microsoft	Microsoft	Serious	UNKNOWN	3
Aug 30 05:28:21 PM	System.dll	Microsoft	Microsoft	Serious	UNKNOWN	3
Aug 30 05:06:22 PM	System.dll	Microsoft	Microsoft	Low	UNKNOWN	2
Aug 30 05:06:22 PM	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
Aug 30 05:06:22 PM	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
Aug 30 05:06:22 PM	System.dll	Microsoft	Microsoft	Serious	UNKNOWN	1
Aug 30 04:48:43 PM	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
Aug 30 04:42:32 PM	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
Aug 30 04:40:15 PM	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
Aug 30 04:28:32 PM	System.dll	Microsoft	Microsoft	Serious	UNKNOWN	1
Aug 30 04:02:10 PM	System.dll	Microsoft	Microsoft	Serious	UNKNOWN	1
Aug 30 03:56:23 PM	System.dll	Microsoft	Microsoft	Serious	UNKNOWN	1
Aug 30 03:52:24 PM	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
Aug 30 03:38:18 PM	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
Aug 30 03:38:18 PM	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
Aug 30 03:38:18 PM	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
Aug 30 01:32:23 PM	System.dll	Microsoft	Microsoft	Low	SAFE	1
Aug 30 01:28:16 PM	System.dll	Microsoft	Microsoft	High	UNKNOWN	1
Aug 30 10:52:11 AM	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
Aug 30 09:54:15 AM	System.dll	Microsoft	Microsoft	Low	UNKNOWN	1
Aug 30 08:46:09 AM	System.dll	Microsoft	Microsoft	Low	UNKNOWN	2
Aug 30 08:46:09 AM	System.dll	Microsoft	Microsoft	Low	UNKNOWN	2
Aug 30 08:46:09 AM	System.dll	Microsoft	Microsoft	Low	UNKNOWN	2
Aug 30 08:12:17 AM	System.dll	Microsoft	Microsoft	High	UNKNOWN	1

Page Size: 25 of 46 GO

Overview

1,217 Action Taken Processes

Acknowledge All

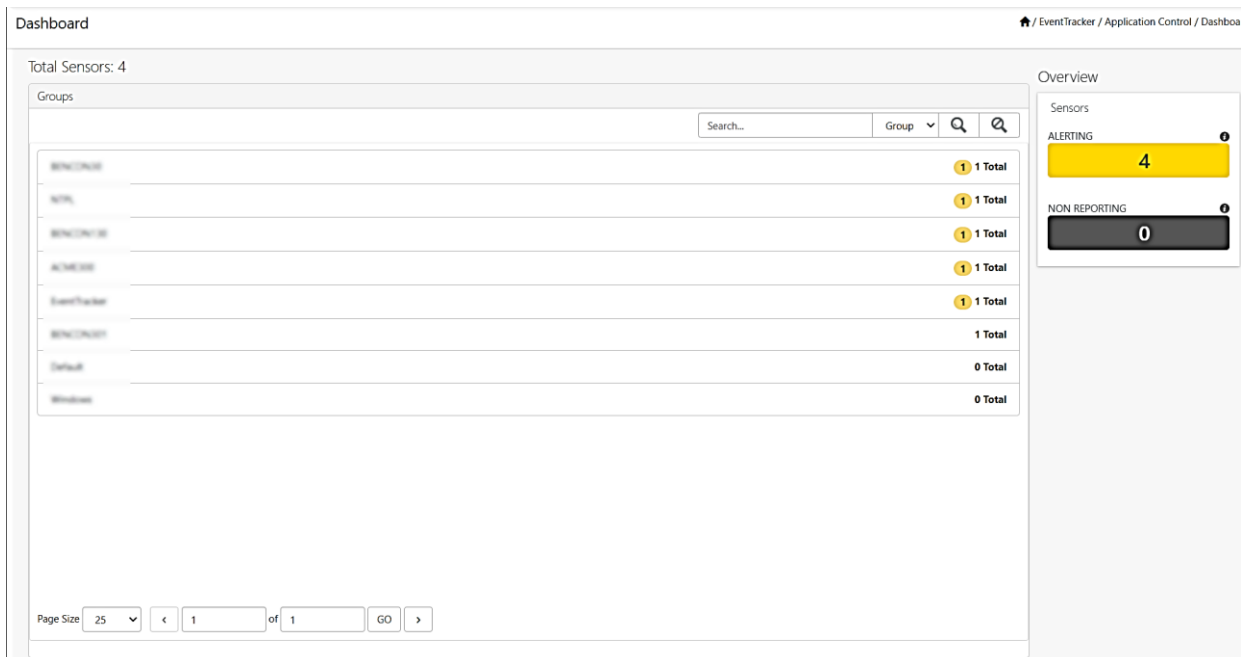
3 Application Control Dashboard

Application Control sensors are installed on the endpoints and are configured on the networks that monitor and record all system-level activities. The Dashboard displays sensor activities across all integrated devices. The Application Control dashboard consists of three panes and displays Overview panels on the right.

The following are the three panes along with Overview panels available in the Application Control Dashboard:

Groups

- **Groups pane:** The Groups pane lists all the available group details. By default, all the groups are displayed in a row.
- **Groups Overview:** The Overview pane located next to the Groups pane displays the sensor/ system activity status of the Group that you select.



Pending Analyst Review

- Pending Analyst Review:** The Pending Analyst Review displays the information of tracking processes, file system and registry modifications like .exe and .dll, that are to be either **Allowed** or **Denied** or **Researched**.
- Pending Analyst Overview:** The **Overview** section located next to the Pending Analyst Review pane provides the details of the number of pending review processes.

Pending Analyst Review:143

File Name
🔍
🔍

<input type="checkbox"/>	File Found Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places
<input type="checkbox"/>	0 minutes ago	SystemInfo.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	1
<input type="checkbox"/>	0 minutes ago	svchost.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	1
<input type="checkbox"/>	0 minutes ago	ipconfig.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	1
<input type="checkbox"/>	2 minutes ago	cmd.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	1
<input type="checkbox"/>	2 minutes ago	Taskmgr.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	1
<input type="checkbox"/>	2 minutes ago	index.html	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	1
<input type="checkbox"/>	2 minutes ago	ipconfig.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	SAFE	1
<input type="checkbox"/>	2 minutes ago	taskmgr.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	1
<input type="checkbox"/>	2 minutes ago	cmd.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	1
<input type="checkbox"/>	4 minutes ago	SECURITY.DLL	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	2
<input type="checkbox"/>	6 minutes ago	Winlogon.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	1
<input type="checkbox"/>	6 minutes ago	lsass.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	SAFE	1
<input type="checkbox"/>	6 minutes ago	authntz.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	1
<input type="checkbox"/>	6 minutes ago	ClientCacheCommonProxyStub.dll	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	1
<input type="checkbox"/>	6 minutes ago	TCShell.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	1
<input type="checkbox"/>	6 minutes ago	services.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	SAFE	2
<input type="checkbox"/>	6 minutes ago	svchost.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	1
<input type="checkbox"/>	8 minutes ago	GoogleUpdate.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	2
<input type="checkbox"/>	8 minutes ago	ipconfig.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	1
<input type="checkbox"/>	10 minutes ago	UserlogProxy.dll	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	1
<input type="checkbox"/>	10 minutes ago	svchost.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	1
<input type="checkbox"/>	10 minutes ago	SystemIdle.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	SAFE	1
<input type="checkbox"/>	10 minutes ago	svchost.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	1
<input type="checkbox"/>	10 minutes ago	csrss.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	1
<input type="checkbox"/>	12 minutes ago	svchost.exe	SENCDN130	ETTHAMBURNN11-SENCDN130	Low	UNKNOWN	1

Page Size

<

of

GO
>

Overview

143 Pending Processes

TERMINATED

0

NOT TERMINATED

143

DORMANT

0

BULK ACTION

Allow All

Deny All

Action Taken Processes

- **Action Taken Processes pane:** The Action Taken Processes pane displays the corrective action to be taken (response) such as **Allowed**, **Denied** or **Researched** against the findings.
- **Action Taken Processes Overview:** The Overview pane located next to the Action Taken Processes pane shows the acknowledgment of all response/corrective actions taken.

Action Taken Processes: 1,147

File Name
Q
Q

	Action Taken Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places	
<input type="checkbox"/>	6 minutes ago	benconhouse.exe	BENCONHOUSE	ETTANBLURBN11-BENCONHOUSE	Low	SAFE	2	⋮
<input type="checkbox"/>	Aug 30 05:28:21 PM	wwwk8r.dll	EventTracker	R100-WR01	Serious	UNKNOWN	3	⋮
<input type="checkbox"/>	Aug 30 05:28:21 PM	crashr.dll	EventTracker	R100-WR01	Serious	UNKNOWN	3	⋮
<input type="checkbox"/>	Aug 30 05:06:22 PM	File_SpringClean.exe	BENCONHOUSE	ETTANBLURBN11-BENCONHOUSE	Low	UNKNOWN	2	⋮
<input type="checkbox"/>	Aug 30 05:06:22 PM	benconhouse.exe	BENCONHOUSE	ETTANBLURBN11-BENCONHOUSE	Low	UNKNOWN	1	⋮
<input type="checkbox"/>	Aug 30 05:06:22 PM	wwwk8r.dll	BENCONHOUSE	ETTANBLURBN11-BENCONHOUSE	Low	UNKNOWN	1	⋮
<input type="checkbox"/>	Aug 30 05:06:22 PM	CRASHR.dll	EventTracker	R100-WR01	Serious	UNKNOWN	1	⋮
<input type="checkbox"/>	Aug 30 04:48:43 PM	BackgroundTransferHost.exe	BENCONHOUSE	ETTANBLURBN11-BENCONHOUSE	Low	UNKNOWN	1	⋮
<input type="checkbox"/>	Aug 30 04:42:22 PM	SLC.dll	BENCONHOUSE	ETTANBLURBN11-BENCONHOUSE	Low	UNKNOWN	1	⋮
<input type="checkbox"/>	Aug 30 04:40:15 PM	wwwk8r.dll	BENCONHOUSE	ETTANBLURBN11-BENCONHOUSE	Low	UNKNOWN	1	⋮
<input type="checkbox"/>	Aug 30 04:28:32 PM	wwwk8r.dll	EventTracker	R100-WR01	Serious	UNKNOWN	1	⋮
<input type="checkbox"/>	Aug 30 04:02:10 PM	wwwk8r.dll	EventTracker	R100-WR01	Serious	UNKNOWN	1	⋮
<input type="checkbox"/>	Aug 30 03:56:23 PM	System.Diagnostics.EventLog.dll	EventTracker	R100-WR01	Serious	UNKNOWN	1	⋮
<input type="checkbox"/>	Aug 30 03:52:24 PM	wwwk8r.dll	BENCONHOUSE	ETTANBLURBN11-BENCONHOUSE	Low	UNKNOWN	1	⋮
<input type="checkbox"/>	Aug 30 03:38:18 PM	SpeechControl.dll	BENCONHOUSE	ETTANBLURBN11-BENCONHOUSE	Low	UNKNOWN	1	⋮
<input type="checkbox"/>	Aug 30 03:38:18 PM	SLC.dll	BENCONHOUSE	ETTANBLURBN11-BENCONHOUSE	Low	UNKNOWN	1	⋮
<input type="checkbox"/>	Aug 30 01:32:23 PM	System.Windows.Common-System.dll	BENCONHOUSE	ETTANBLURBN11-BENCONHOUSE	Low	SAFE	1	⋮
<input type="checkbox"/>	Aug 30 01:20:16 PM	configmgragent.dll	ACME300	W7P276L300-ACME300	High	UNKNOWN	1	⋮
<input type="checkbox"/>	Aug 30 10:52:11 AM	wwwk8r.dll	BENCONHOUSE	ETTANBLURBN11-BENCONHOUSE	Low	UNKNOWN	1	⋮
<input type="checkbox"/>	Aug 30 09:54:15 AM	CRASHR.dll	BENCONHOUSE	ETTANBLURBN11-BENCONHOUSE	Low	UNKNOWN	1	⋮
<input type="checkbox"/>	Aug 30 08:46:09 AM	wwwk8r.dll	BENCONHOUSE	ETTANBLURBN11-BENCONHOUSE	Low	UNKNOWN	2	⋮
<input type="checkbox"/>	Aug 30 08:46:09 AM	wwwk8r.dll	BENCONHOUSE	ETTANBLURBN11-BENCONHOUSE	Low	UNKNOWN	2	⋮
<input type="checkbox"/>	Aug 30 08:46:09 AM	GoogleUpdate.exe	BENCONHOUSE	ETTANBLURBN11-BENCONHOUSE	Low	UNKNOWN	2	⋮
<input type="checkbox"/>	Aug 30 08:46:09 AM	crashr.dll	BENCONHOUSE	ETTANBLURBN11-BENCONHOUSE	Low	UNKNOWN	2	⋮
<input type="checkbox"/>	Aug 30 08:12:17 AM	MPHMLP.dll	ACME300	W7P276L300-ACME300	High	UNKNOWN	1	⋮

Page Size
25
<
1
of
46
GO
>

Overview

1217 Action Taken Processes

Acknowledge All

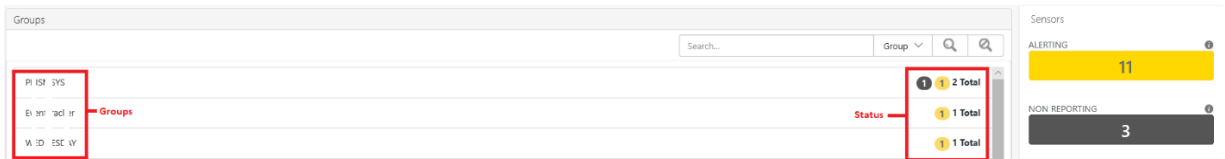
3.1 Groups Pane

In this pane, by default all the Groups are listed in a row. You can view events and activities of the systems/sensors through search function.

- Click the **Search** drop-down list and select either **Group** or **Sensor** to filter and view the status.
- In the **Search** field, type in the name of a Group or a Sensor to perform an individual search.



- Each color indicates a Group status.






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

Color	Status	Description
Yellow 1	ALERTING	This status indicates all the locations or systems where a new process has appeared.
Gray 1	NON-REPORTING	This status indicates that a 'keep alive' status is not received from the systems or locations.

- To view a specific group status, click the individual Group and it expands to display the sensors, and the process status of the sensors.



- 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 Netsurion Application Control.
Fountain Blue 	NOT TERMINATED	Indicates the process that ran during the maintenance mode and is now running without disposition.

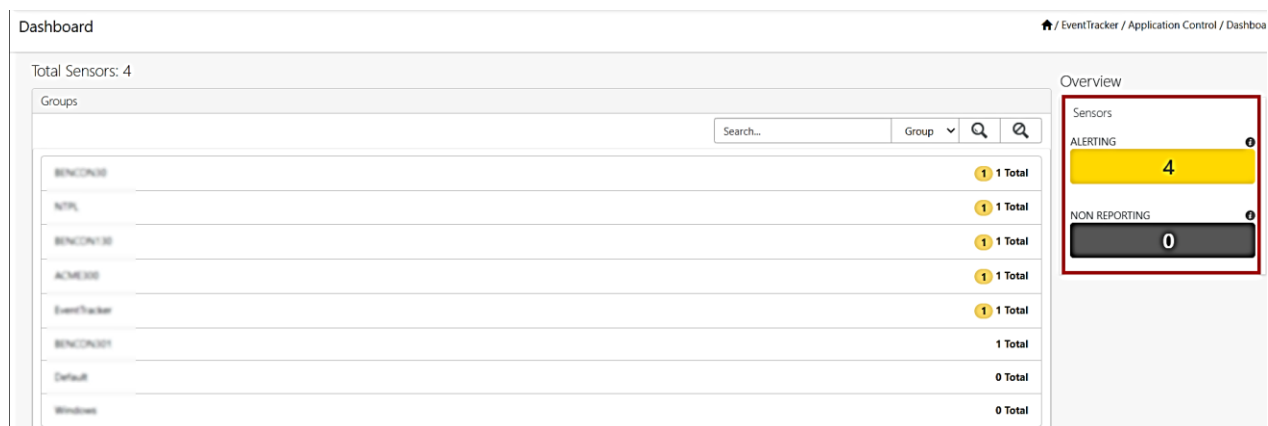
- When you click the color icons, it filters the Application Control database and displays all the events of that status in the **Pending Analyst Review pane**.



For example, when you click the orange icon, the details of all the dormant processes in the **Pending Analyst Review pane** will be displayed.



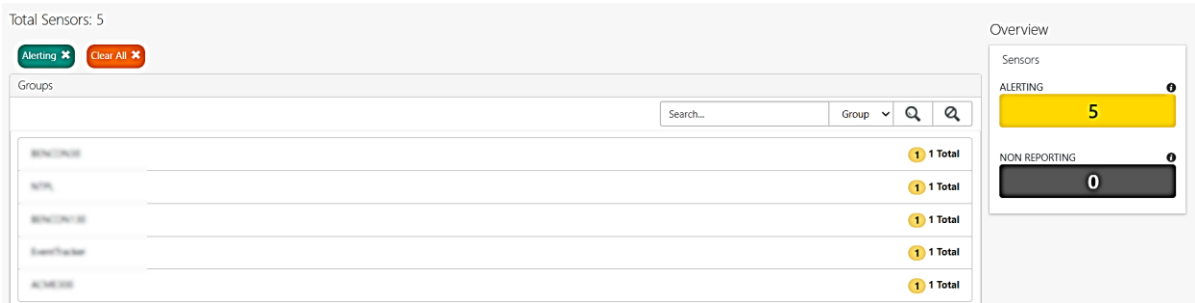
3.1.1 Groups Overview

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

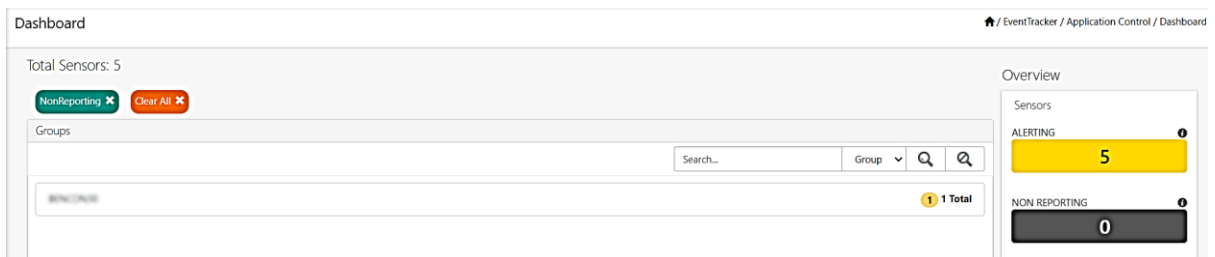


Color	Status	Description
Yellow 	ALERTING	This status shows all the locations or systems where a new process has appeared.
Gray 	NON-REPORTING	This status shows not received a 'keep alive' status from the systems or locations.

- **ALERTING:** Click **Alerting**, to view all the groups with Alert status in the Groups pane. It filters the Application Control database and displays all the events of that status.



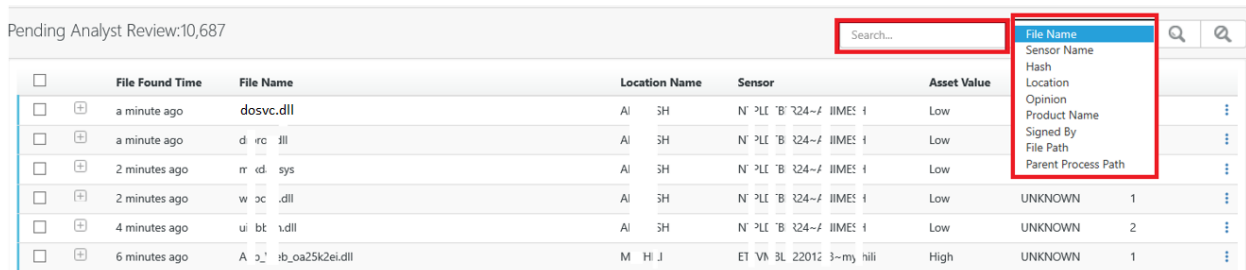
- **NON-REPORTING:** Click **non-reporting**, to view all groups with non-reporting status in the Groups pane. It filters the Application Control database and displays all the events of that status.



3.2 Pending Analyst Pane

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

- The search can be performed by **File Name, Sensor Name, Hash, Location, Opinion, Product Name, Signed By, File Path, and Parent Process Path.**
- Based on the search results, the status of the sensors will be displayed.



- You can select either **Allow**, or **Deny**, or **Research** action to achieve the appropriate endpoint policies.
- Select the required process and click the **tools** button to choose either **Allow**, or **Deny**, or **Research**.

Note

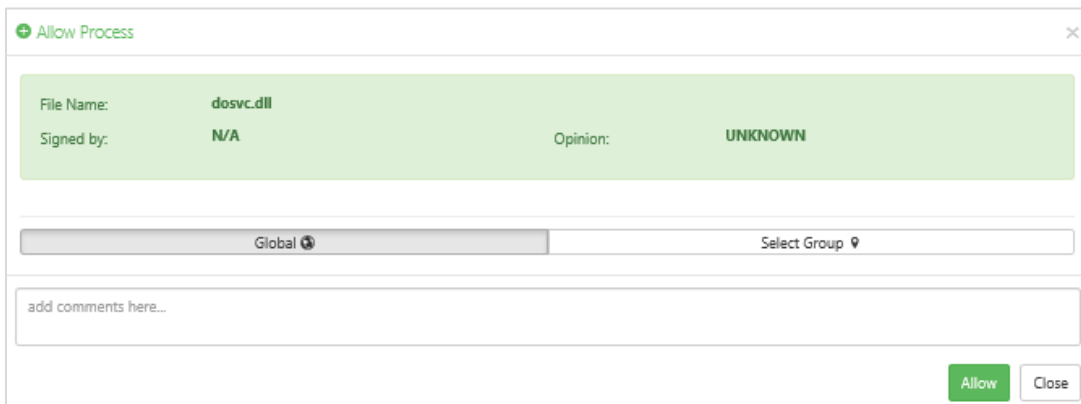
Events/ Incidents pending in the Analyst pane for 3 days without any action will be automatically moved to **Research**. Action taken Events/Incidents will be moved to the **Action Taken processes** pane.

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	PLDT^R30-V^edn day	Low	UNKNOWN	Allow
<input type="checkbox"/>	6 minutes ago	NTL MNMA .DLL	NIME iH	PLDT R24-f NIMI iH	Low	UNKNOWN	Deny
<input type="checkbox"/>	6 minutes ago	drp sv.dll	NIME iH	PLDT R24-f NIMI iH	Low	UNKNOWN	Research
<input type="checkbox"/>	7 minutes ago	mrx lav.sv	NIME iH	PLDT R24-f NIMI iH	Low	UNKNOWN	1
<input type="checkbox"/>	7 minutes ago	wet 3nt.dll	NIME iH	PLDT R24-f NIMI iH	Low	UNKNOWN	1
<input type="checkbox"/>	9 minutes ago	uirit bon.d	NIME iH	PLDT R24-f NIMI iH	Low	UNKNOWN	2
<input type="checkbox"/>	11 minutes ago	App_Web_ i25k2ei.dll	YTHI J	IVME i22012 3-n thili	High	UNKNOWN	1
<input type="checkbox"/>	11 minutes ago	App_Web_ ykmiqh.dll	YTHI J	IVME i22012 3-n thili	High	UNKNOWN	1
<input type="checkbox"/>	11 minutes ago	msj toledt 0.dll	YTHI J	IVME i22012 3-n thili	High	UNKNOWN	3
<input type="checkbox"/>	11 minutes ago	QUI TY.DLI	NIME iH	PLDT R24-f NIMI iH	Low	SAFE	2
<input type="checkbox"/>	12 minutes ago	App_Web_ 1puo2et.dll	YTHI J	IVME i22012 3-n thili	High	UNKNOWN	1

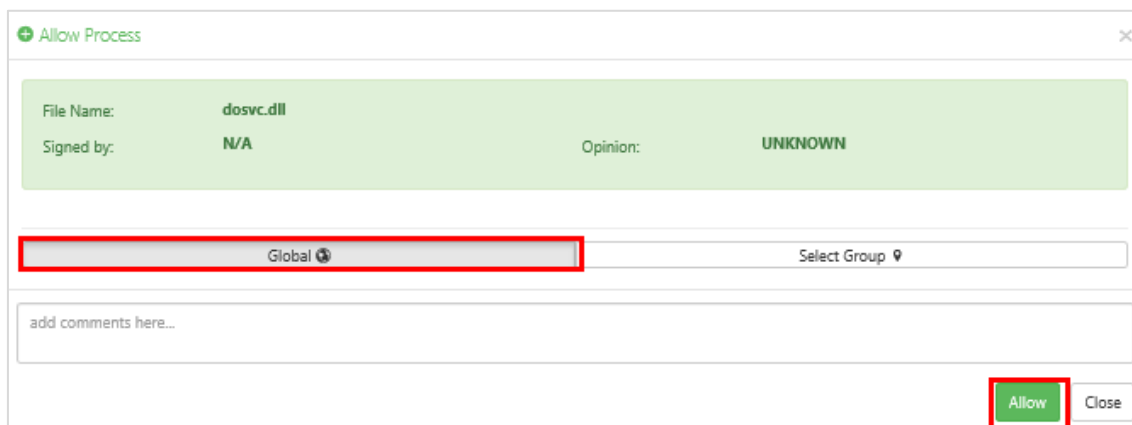
Allowing the process

1. If you click **Allow**, the **Allow Process** window pops-up.

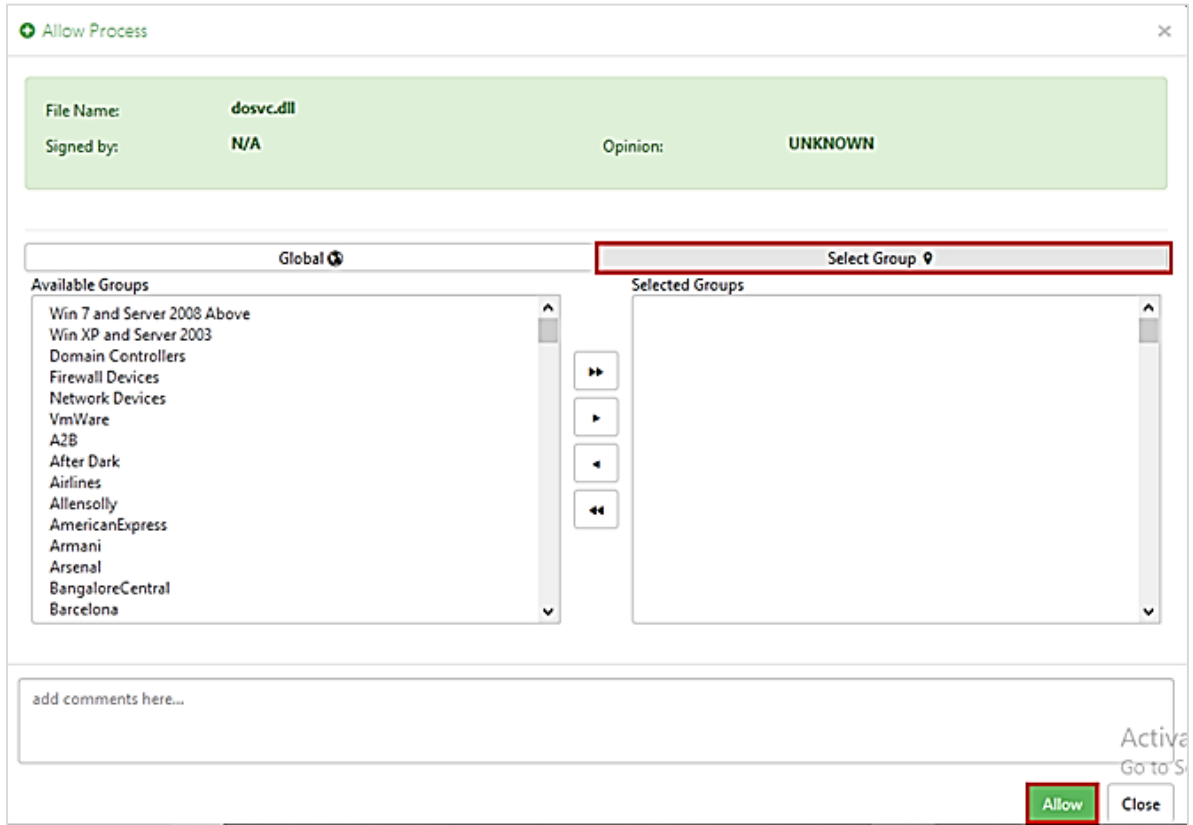


2. Select either **Global** or **Select Group** option to select the environment and click **Allow**.

- Selecting the **Global** option selects all the groups in the environment.

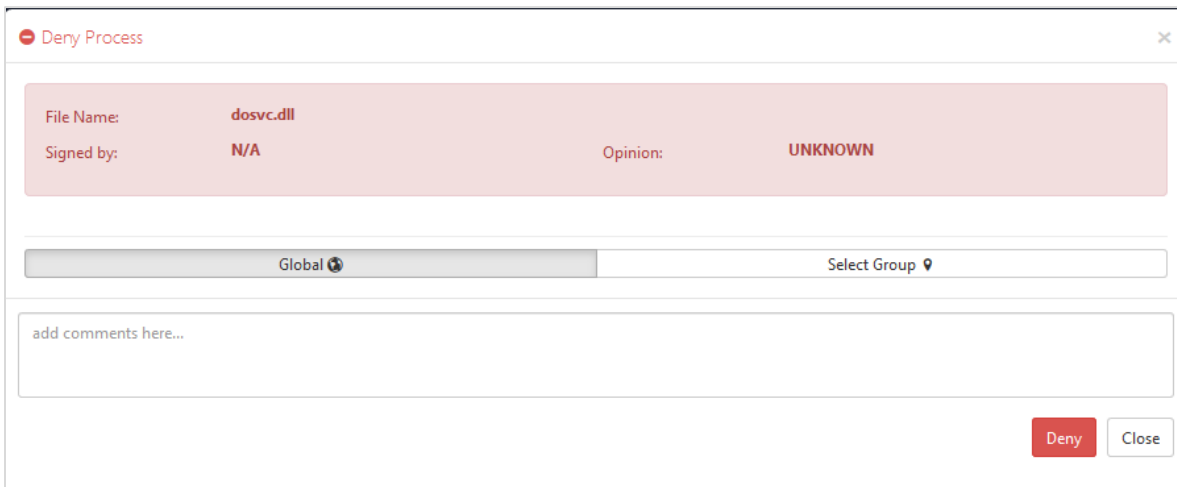


- Selecting the **Select Group** option allows to select the required groups from the **Available Groups** list.



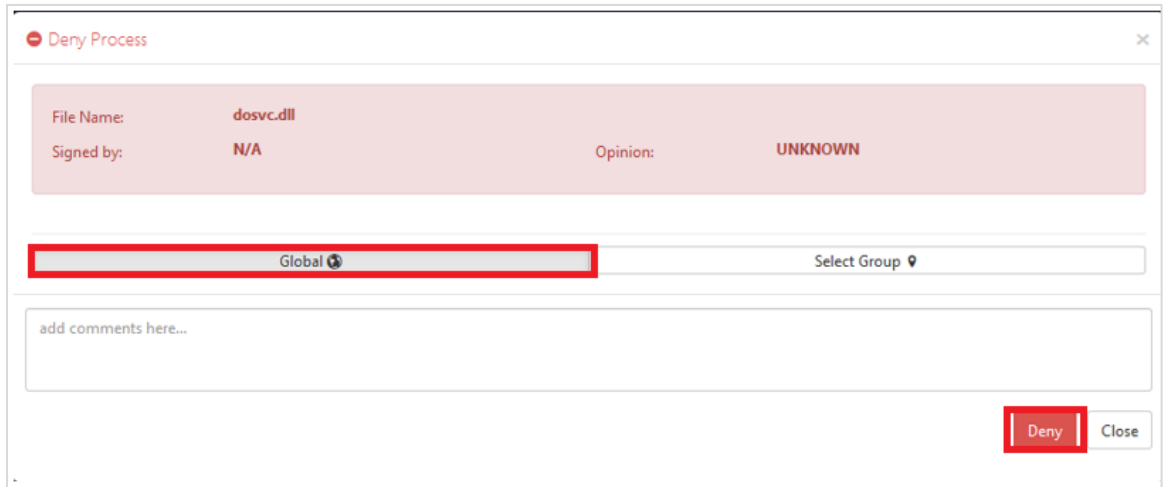
Denying the process

1. If you click **Deny** the Deny Process window pops-up.

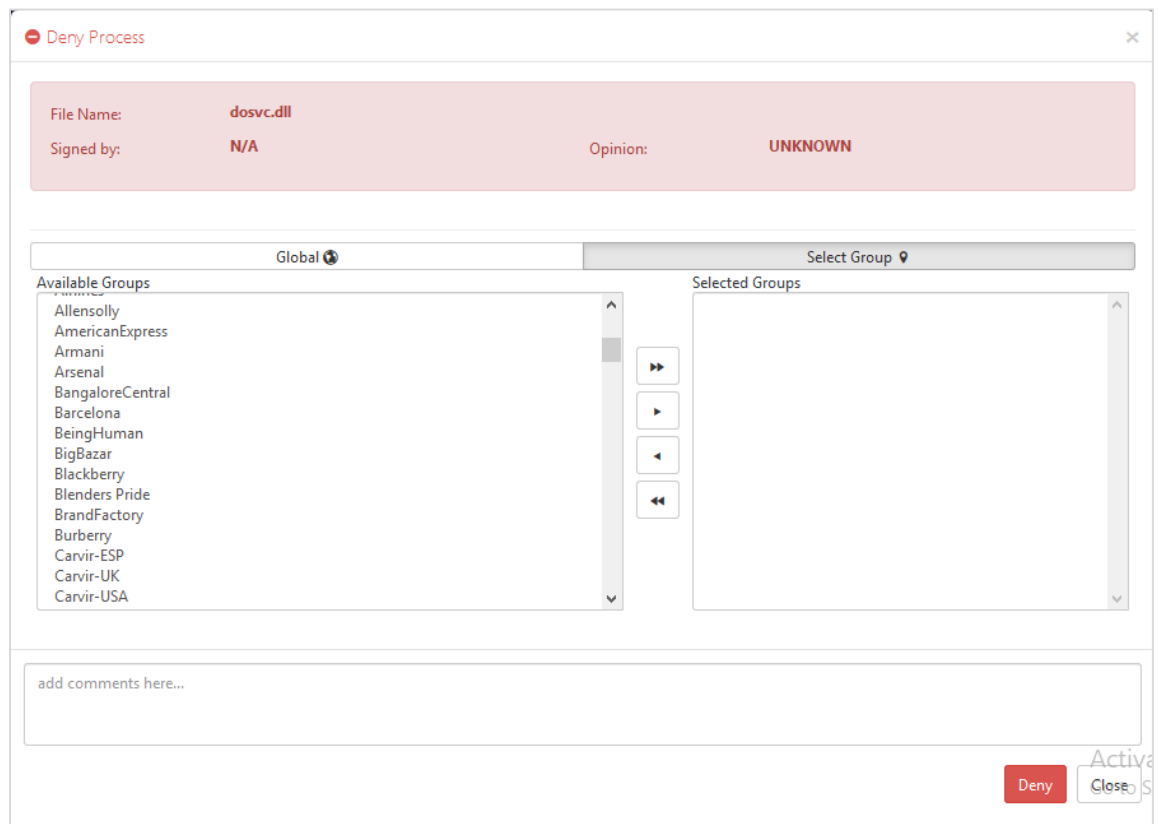


2. Select either **Global** or **Select Group** option to deny the environment and click **Deny**.

- Selecting the **Global** option selects all the groups in the environment to deny.




- Selecting the **Select Group** option allows to deny only the selected groups from the **Available Groups** list.



Detailed View of Pending Analyst Review Pane

All the processes requiring review are displayed in the Pending Analyst Review Pane. Perform the following to view a process detail,

- In the **Pending Analyst Review** pane, go to the required process in the list and click the **expand**  button located before the process in the list.

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="checkbox"/>	6 minutes ago	NTL WNMA .DLL	NIME JH	N PLDT R24~f NIMI H	Low	UNKNOWN
<input type="checkbox"/>	6 minutes ago	drpi xv.dll	NIME JH	N PLDT R24~f NIMI H	Low	UNKNOWN
<input type="checkbox"/>	7 minutes ago	mrx lav.sys	NIME JH	N PLDT R24~f NIMI H	Low	UNKNOWN
<input type="checkbox"/>	7 minutes ago	wel jnt.dll	NIME JH	N PLDT R24~f NIMI H	Low	UNKNOWN
<input type="checkbox"/>	9 minutes ago	uirit bon.d	NIME JH	N PLDT R24~f NIMI H	Low	UNKNOWN
<input type="checkbox"/>	11 minutes ago	App _Web_ i25k2ei.dll	YTHI J	E IVME i2201z 3~n thili	High	UNKNOWN
<input type="checkbox"/>	11 minutes ago	App _Web_ ykmiqh.dll	YTHI J	E IVME i2201z 3~n thili	High	UNKNOWN
<input type="checkbox"/>	11 minutes ago	msj toledt 0.dll	YTHI J	E IVME i2201z 3~n thili	High	UNKNOWN
<input type="checkbox"/>	11 minutes ago	QUJ Y.DLI	NIME JH	N PLDT R24~f NIMI H	Low	SAFE
<input type="checkbox"/>	12 minutes ago	App _Web_ i3puo2et.dll	L.YTHI J	E IVME i2201z 3~n thili	High	UNKNOWN

- The tab expands to provide a detailed view of that particular process.

Pending Analyst Review:21,401

6 hours ago dstokenclean.exe

Thane, 400606
IP Address 172.28.9.164
Log Time Sep 01 07:57:18 AM
Computer ETTVMBLR2W10-2
Contact

Launched by:
Domain NT AUTHORITY
User Name SYSTEM

Observation
Process does not match the allowed process criteria.

1 File Names

File Version 10.0.17763.1
Product Name Microsoft® Windows® Operating System
Signed By
Counter Signed By N/A
Signed On
File Modified Time Sep 01 07:57:18 AM
Parent Process Name svchost.exe
Parent Process Path C:\Windows\System32\svchost.exe
Parent Process Hash 23e47ce30cfc49f60a6e24b50aa83b9b
File Path C:\Windows\system32\dstokenclean.exe
Hash 6a7d8561bcba33ed64e3befd67c10ca0

Detected on sensors 2

ETTVMBLR2W10-2 6 hours ago
ETTVMBLR22019-44aug 17 06:23:44 PM

Overview

21,401 Pending Processes

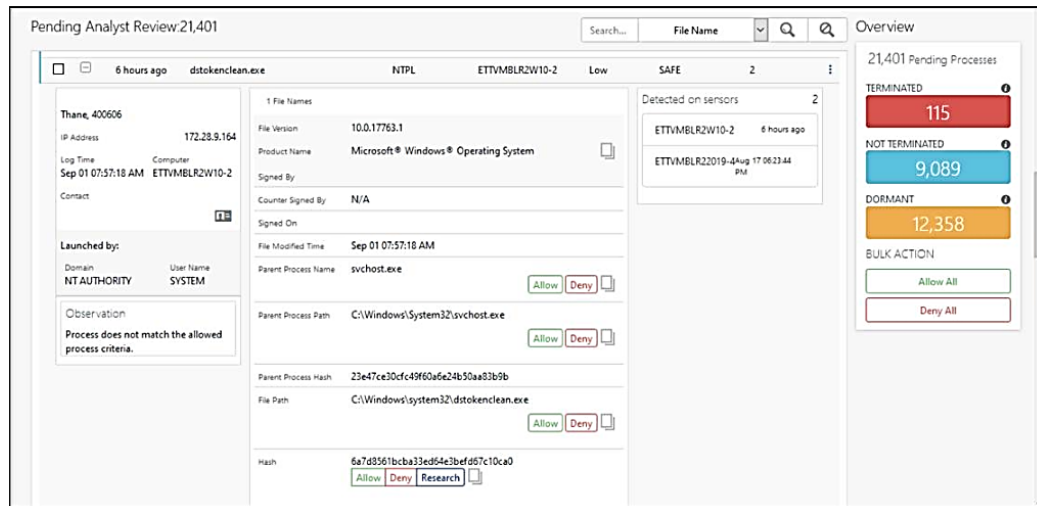
TERMINATED 115

NOT TERMINATED 9,089

DORMANT 12,358

BULK ACTION

The process in the Pending Analyst Review pane can also be allowed or denied using the following filters.



1. **Parent Process Name** - Click either **Allow** or **Deny** if you require to allow or deny the process by Parent Process name.

For example,

If the **w3wp.exe** process is allowed along with the parent process name and whenever w3wp.exe process is detected with the same parent process name, it will be automatically considered as safe.

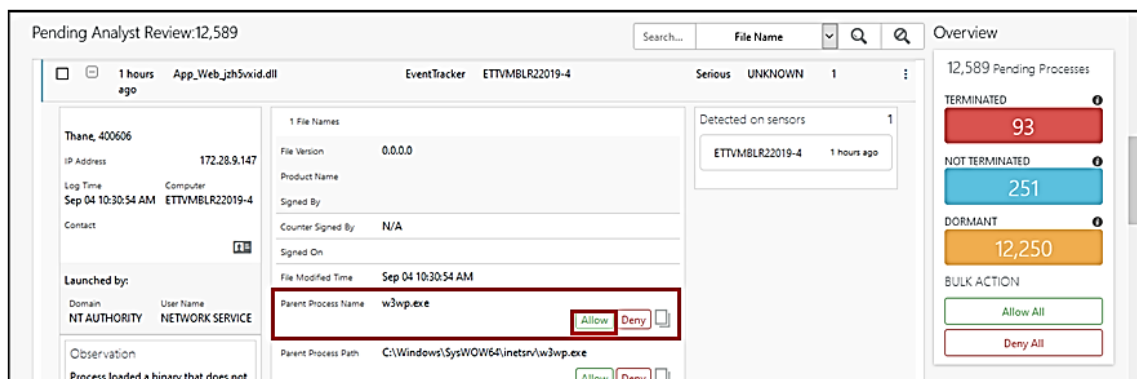
2. **Parent Process Path** - Click either **Allow** or **Deny** if you require to allow or deny the process by parent process path.
3. **Parent Process Hash** – Every Parent Process Name includes a Parent Process Hash value.

For example,

If the **w3wp.exe** process was **ALLOWED** with a Parent Process name along with the particular Parent Process Hash value (for example, abc) but instead, detected with a different Parent Process Hash value (for example, xyz), then it will not be considered **SAFE**.

In this case, it is required to select the appropriate action (**Allow** or **Deny**) again.

- If you require to allow the **Parent Process Name** with the different **Parent Process Hash** value, click **Allow** to fetch the **Parent Process Hash** value.



- In the **Add rule** window, specify the appropriate details, and click **Add** to include the Hash to the process.

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

4. **File path** - Click either **Allow** or **Deny** if you require to allow or deny the process by file path.
5. **Hash** - Click either **Allow** or **Deny** if you require to allow or deny the process by hash. Click **Research** if you require to analyze the particular Hash.

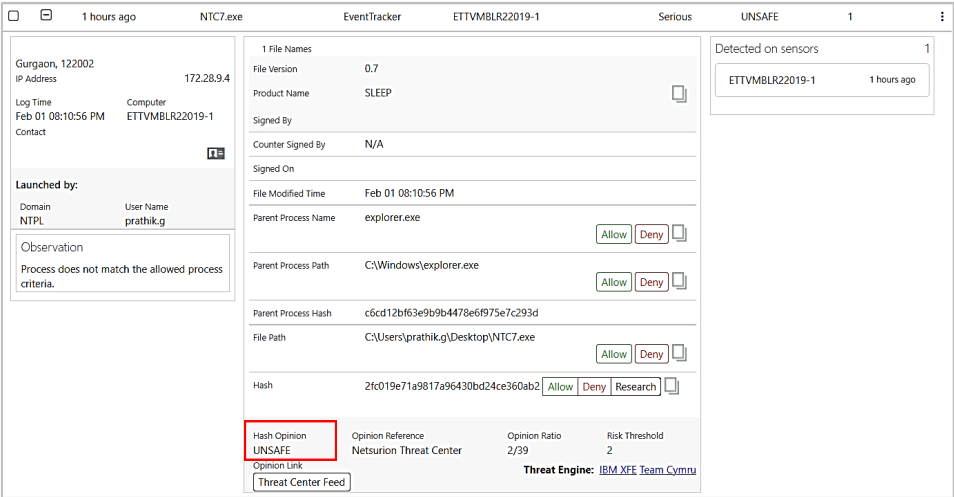
- **Hash Opinion** - The Netsurion Threat Center provides opinion for Hash, that is, whenever a process is detected, the corresponding Hash lookup will first take place from the **Netsurion Threat Centre**.
- **Opinion Reference:** Displays the name of the service provider that performed the hash lookup, such as **Netsurion Threat Center** or any other service provider like Virus Total, and more.

Note:

The Netsurion Threat Center Platform is an alternate Hash reputation provider that determines the badness/reputation of the Hash. It accumulates a series of different threat feeds, gathers information about the Hash details, scans the detected Hash value with multiple other Hash details to find the security threats.

- **Opinion Ratio:** The number of feeds that have flagged the hash as unsafe is provided by Opinion Ratio.
- **Risk Threshold:** The limit value that, when met or exceeded, is regarded as unsafe.

The Netsurion Threat Center provides the following Opinions.

<p>Hash Opinion UNSAFE</p>	<p>If the Hash is found unsafe in the Netsurion Threat Center, then the Hash opinion is provided as UNSAFE.</p> 
<p>Hash Opinion UNKNOWN</p>	<p>The Hash opinion is specified as UNKNOWN if the Hash is not available in the Netsurion Threat Center, is neither found to be UNSAFE nor below the Threshold value, and a lookup from Virus Total is not possible.</p>

EventTracker | ETTVMBLR22019-1 | Serious | UNKNOWN | 1

Host Information:
 Gurgaon, 122002 | IP Address: 172.28.9.4
 Log Time: Feb 01 06:07:50 PM | Computer: ETTVMBLR22019-1
 Contact: [redacted]

Launched by:
 Domain: NTPL | User Name: prathik.g

Observation:
 Process does not match the allowed process criteria.

File Details:
 1 File Names
 File Version: 1.8 | Product Name: SLEEP
 Signed By: [redacted]
 Counter Signed By: N/A | Signed On: [redacted]
 File Modified Time: Feb 01 06:07:50 PM
 Parent Process Name: explorer.exe [Allow] [Deny] [Copy]
 Parent Process Path: C:\Windows\explorer.exe [Allow] [Deny] [Copy]
 Parent Process Hash: c6cd12bf63e9b9b4478e6f975e7c293d
 File Path: C:\Users\prathik.g\Desktop\NTC18.exe [Allow] [Deny] [Copy]
 Hash: bacc54cbedff0173d0fada27d09680a [Allow] [Deny] [Research] [Copy]

Opinion Summary:
 Hash Opinion: UNKNOWN | Opinion Reference: Netsurion Threat Center | Opinion Ratio: 0/0 | Risk Threshold: 1 | Opinion Link: [redacted]
 Threat Engine: IBM.XFE Team_Cymru

Detected on sensors:
 ETTVMBLR22019-1 | a minute ago

- Opinion Link:** In the **Opinion Link**, click the **Threat Center Feed** button to see the feed source details.

EventTracker | ETTVMBLR22019-1 | Serious | UNSAFE | 1

Host Information:
 Gurgaon, 122002 | IP Address: 172.28.9.4
 Log Time: Feb 01 08:10:56 PM | Computer: ETTVMBLR22019-1
 Contact: [redacted]

Launched by:
 Domain: NTPL | User Name: prathik.g

Observation:
 Process does not match the allowed process criteria.

File Details:
 1 File Names
 File Version: 0.7 | Product Name: SLEEP
 Signed By: [redacted]
 Counter Signed By: N/A | Signed On: [redacted]
 File Modified Time: Feb 01 08:10:56 PM
 Parent Process Name: explorer.exe [Allow] [Deny] [Copy]
 Parent Process Path: C:\Windows\explorer.exe [Allow] [Deny] [Copy]
 Parent Process Hash: c6cd12bf63e9b9b4478e6f975e7c293d
 File Path: C:\Users\prathik.g\Desktop\NTC7.exe [Allow] [Deny] [Copy]
 Hash: 2fc019e71a9817a96430bd24ce360ab2 [Allow] [Deny] [Research] [Copy]

Opinion Summary:
 Hash Opinion: UNSAFE | Opinion Reference: Netsurion Threat Center | Opinion Ratio: 2/39 | Risk Threshold: 2 | Opinion Link: [redacted]
 Threat Engine: IBM.XFE Team_Cymru

Opinion Link:
 Threat Center Feed

Detected on sensors:
 ETTVMBLR22019-1 | 1 hours ago

Threat Center Feed Source Details

Threat Center Feed

- Hash Events
- Hash Unsafe Events

Close

- **Threat Engine:** Click the respective **Threat Engine Lookup Service provider** hyperlink to look for more information on the Hash.

1 hours ago NTC7.exe EventTracker ETTVMBLR22019-1 Serious UNSAFE 1

Gurgaon, 122002
IP Address 172.28.9.4
Log Time Feb 01 08:10:56 PM Computer ETTVMBLR22019-1
Contact

Launched by:
Domain User Name
NTPL prathik.g

Observation
Process does not match the allowed process criteria.

1 File Names
File Version 0.7
Product Name SLEEP
Signed By
Counter Signed By N/A
Signed On
File Modified Time Feb 01 08:10:56 PM
Parent Process Name explorer.exe
Parent Process Path C:\Windows\explorer.exe
Parent Process Hash c6cd12bf63e9b9b4478e6f975e7c293d
File Path C:\Users\prathik.g\Desktop\NTC7.exe
Hash 2fc019e71a9817a96430bd24ce360ab2
Hash Opinion UNSAFE
Opinion Reference Netsurion Threat Center
Opinion Ratio 2/39
Risk Threshold 2
Threat Engine: IBM XFE Team Cymru

Detected on sensors
ETTVMBLR22019-1 1 hours ago

When the respective Hash is not found in the Netsurion Threat Center then the lookup will happen from **Virus Total** which provides the following Opinions.

	<p>Hash found unsafe from Virus Total.</p> <p>25 minutes ago Vaccine3.exe EventTracker ETTVMBLR22019-1 Serious UNSAFE 1</p> <p>Gurgaon, 122002 IP Address 172.28.9.4 Log Time Feb 01 06:19:51 PM Computer ETTVMBLR22019-1 Contact</p> <p>Launched by: Domain User Name NS5 PK5</p> <p>Observation Process does not match the allowed process criteria.</p> <p>1 File Names File Version 0.6 Product Name SLP01 Signed By Counter Signed By N/A Signed On File Modified Time Feb 01 06:19:51 PM Parent Process Name explorer.exe Parent Process Path C:\Windows\explorer.exe Parent Process Hash f070b5cf25febb9a88a168efd87c6112 File Path C:\Users\prathik.g\Desktop\Vaccine3.exe Hash b1563f567dd1922f27f7d0b300c27d2b Hash Opinion UNSAFE Opinion Reference VirusTotal Opinion Ratio 42/56 Threat Engine: IBM XFE Team Cymru</p> <p>Detected on sensors ETTVMBLR22019-1 25 minutes ago</p>
<p>Hash Opinion UNSAFE</p>	<p>Hash found safe from Virus Total.</p>

**Hash
Opinion
UNKNOWN**

14 minutes ago NET1.EXE EventTracker ETTVMBLR22019-1 Serious SAFE 1

Gurgaon, 122002
IP Address 172.28.9.4
Log Time Feb 20 12:55:47 PM Computer ETTVMBLR22019-1
Contact

Launched by:
Domain NT AUTHORITY User Name SYSTEM

Observation
Process does not match the allowed process criteria.

1 File Names

File Version 10.0.17763.1
Product Name Microsoft® Windows® Operating System
Signed By
Counter Signed By N/A
Signed On
File Modified Time Feb 20 12:55:47 PM
Parent Process Name netLexe Allow Deny
Parent Process Path C:\Windows\SysWOW64\netLexe Allow Deny
Parent Process Hash cb0744aa7acb8b8a960f3ce3259739ec
File Path C:\Windows\SysWOW64\netLexe Allow Deny
Hash e28124df01ca79fd93fb7c48decdac0 Allow Deny Research

Hash Opinion	Opinion Reference	Opinion Ratio
SAFE	VirusTotal	0/69

Opinion Link
<https://www.virustotal.com/gui/file/383ecc5dbcd98163c556ca6e4486c5dc6a35c3f1cff88dcf12da2cdaba80970/detection/f-383ecc5dbcd98163c556ca6e4486c5dc6a35c3f1cff88dcf12da2cdaba80970-1675690895>

Threat Engine: IBM.XFE Team Cymru

Detected on sensors 1

ETTVMBLR22019-1 14 minutes ago

a minute ago NTC17.exe EventTracker ETTVMBLR22019-1 Serious UNKNOWN 1

Gurgaon, 122002
IP Address 172.28.9.4
Log Time Feb 01 04:46:58 PM Computer ETTVMBLR22019-1
Contact

Launched by:
Domain NTPL User Name prathik.g

Observation
Process does not match the allowed process criteria.

1 File Names

File Version 1.7
Product Name SLEEPIA
Signed By
Counter Signed By N/A
Signed On
File Modified Time Feb 01 04:46:58 PM
Parent Process Name explorer.exe Allow Deny
Parent Process Path C:\Windows\explorer.exe Allow Deny
Parent Process Hash c6cd12b63e9b9b4478e6975e7c293d
File Path C:\Users\prathik.g\Desktop\NTC17.exe Allow Deny
Hash d7e188ff6dbf8b66ff4238af2030fb2 Allow Deny Research

Hash Opinion	Opinion Reference	Opinion Ratio	Opinion Link
UNKNOWN	VirusTotal	0/0	www.virustotal.com

Threat Engine: IBM.XFE Team Cymru

Detected on sensors 1

ETTVMBLR22019-1 a minute ago

3.2.1 Pending Analyst Overview

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

The screenshot shows the 'Pending Analyst Review: 840' interface. It features a table with columns: File Found Time, File Name, Location Name, Sensor, Asset Value, Opinion, and Places. The table lists various files like 'spcc.dll', 'SLC.dll', 'wininit.dll', 'kbdsu.dll', 'SKS.DLL', 'plopin.dll', 'AppxAllUserStore.dll', 'workful.dll', 'LanguageOverlayServer.dll', and 'WFPNFPFLX'. To the right, an 'Overview' panel displays: 0 Terminated (red), 810 Not Terminated (blue), and 30 Dormant (orange). It also includes 'BULK ACTION' buttons for 'Allow All' and 'Deny All'.

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

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

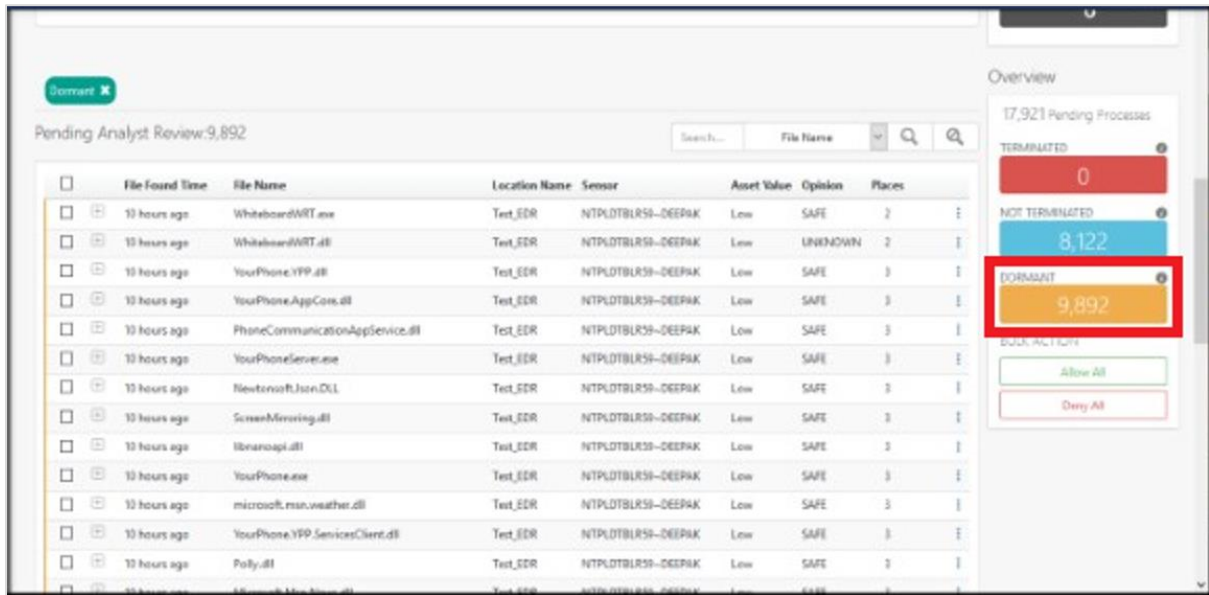
- TERMINATE:** Click the **TERMINATE** tab, to view all the terminated processes in the Analyst Review pane. It filters the Application Control database and displays all the events of that status.

The screenshot shows the 'Pending Analyst Review: 0' interface with the 'Terminated' tab selected. The table is empty. The 'Overview' panel on the right shows: 0 Terminated (red), 463 Not Terminated (blue), and 0 Dormant (orange). 'BULK ACTION' buttons for 'Allow All', 'Deny All', and 'Acknowledge All' are visible.

- NOT TERMINATED:** Click the **NON-TERMINATED** tab, to view all the non-terminated processes in the Analyst Review pane. It filters the Application Control database and displays all the events of that status.

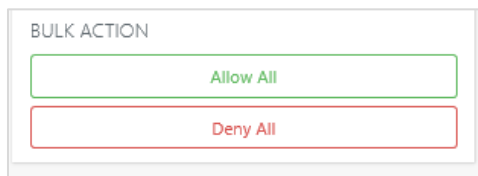
The screenshot shows the 'Pending Analyst Review: 310' interface with the 'Not Terminated' tab selected. The table lists files like 'NOTEPAD.EXE', 'System.Runtime.dll', 'spcc.dll', 'SLC.dll', 'wininit.dll', 'kbdsu.dll', 'SKS.DLL', and 'plopin.dll'. The 'Overview' panel on the right shows: 0 Terminated (red), 810 Not Terminated (blue), and 30 Dormant (orange). 'BULK ACTION' buttons for 'Allow All' and 'Deny All' are visible.

- **DORMANT:** Click the **DORMANT** tab, to view all the dormant processes in the Analyst Review pane. It filters the Application Control database and displays all the events of that status.

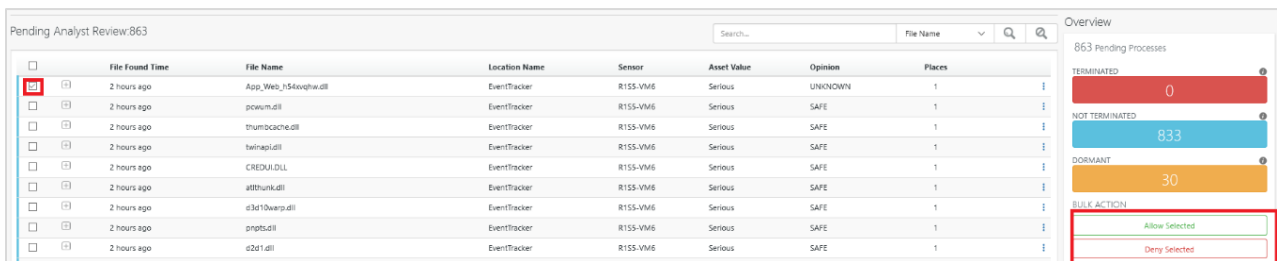


BULK ACTION

- In the **Bulk Action**, click either **Allow All** or **Deny All** button to allow or deny all the processes.



- To select the individual process, click the check box as shown in the following figure.
- In the **Bulk Action**, click **Allow Selected** to allow or click **Deny selected** to deny the selected process.



3.3 Action Taken Processes Pane

This pane displays all the processes for which the necessary actions were taken.

Perform the search by **File Name**, **Sensor Name**, **Hash**, **Location**, **Opinion**, **Product Name**, **Signed By**, **File Path**, **Parent Process Path**, **Parent Process Name**, and **Parent Process Hash**.

The screenshot shows the 'Action Taken Processes' pane with 3,888 processes. A search dropdown menu is open, highlighting 'File Name'. The table below shows the first few rows of the process list:

Action Taken Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places
21 hours ago	MSSPH.DLL	CHETHAN	NTPLDTBLR30~Chethan			
21 hours ago	ShellCommonCommonProxyStub.dll	CHETHAN	NTPLDTBLR30~Chethan			
21 hours ago	NOTEPAD.EXE	MONDAY	R1S3VM2~MONDAY			
22 hours ago	inputswitch.dll	NTPL	NTPLDTBLR81			
22 hours ago	schtasks.exe	ANIMESH	NTPLDTBLR24.ntpl.local~ANIMESH			
Aug 22 06:32:49 AM	dinput8.dll	CHETHAN	NTPLDTBLR30~Chethan			
Aug 22 06:32:48 AM	CRYPTUI.DLL	CHETHAN	NTPLDTBLR30~Chethan			
Aug 22 06:32:47 AM	WS2HELP.DLL	CHETHAN	NTPLDTBLR30~Chethan	Low	SAFE	1
Aug 22 06:32:46 AM	comres.dll	CHETHAN	NTPLDTBLR30~Chethan	Low	SAFE	1
Aug 22 04:23:44 AM	DEFRAG.EXE	EventTracker	ETTVMBLR22019-4	Serious	SAFE	1
Aug 22 04:23:44 AM	defragsvc.dll	EventTracker	ETTVMBLR22019-4	Serious	SAFE	1

1. Click the **expand** button to expand the tab and view the File Names and the corrective action taken.

The screenshot shows the expanded 'Action Taken Processes' pane with 1 process. The process entry is highlighted with a red box:

Action Taken Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places
Apr 03 04:07:34 PM	Wldap32.dll	Default	R1S5-VM9	Low	SAFE	1

The screenshot shows the expanded 'Action Taken Processes' pane with detailed information for the selected process. The 'Detected on sensors' section is highlighted with a red box:

Action Taken Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places
Apr 03 04:07:34 PM	Wldap32.dll	Default	R1S5-VM9	Low	SAFE	1

1 FILE NAMES

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: Apr 03 04:07:34 PM

FILE PATH: C:\Windows\System32\Wldap32.dll

PARENT PROCESS NAME: svchost.exe

PARENT PROCESS PATH: C:\Windows\System32\svchost.exe

MD5 CHECKSUM: 5da293fe9bbabdef5b3874a137ba86cd

HASH OPINION: SAFE

OPINION REFERENCE: VirusTotal

VIRUSTOTAL RATIO: 0/65

VIRUSTOTAL LINK: <https://www.virustotal.com/file/4a261afbcd280d2457dd974ac5ddff18eb866b46015f391a513dc6172b0f1926f/analysis/1554157960/>

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

Detected on sensors: 1

R1S5-VM9 18 Min ago

Buttons: Acknowledge, Allow, Deny, Research

2. Click **Deny** or **Research** in the Action Taken processes window to deny or to further investigate.

3. Click **View Now** to display **Action taken history** of the user and the provided comments.

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

3.3.1 Action Taken Processes Overview

The Overview panel provides the overall visibility of **Action Taken** Process.

- Click **Acknowledge All**, to acknowledge all the processes in the **Action Taken** Process tab.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
 Trade Centre South
 100 W. Cypress Creek Rd
 Suite 530
 Fort Lauderdale, FL 33309

Contact Numbers

Direct Enterprise	SOC@Netsurion.com	1 (877) 333-1433 Option 1, Option 1
MSP Enterprise	SOC-MSP@Netsurion.com	1 (877) 333-1433 Option 1, Option 2
Essentials	Essentials-Support@Netsurion.com	1 (877) 333-1433 Option 1, Option 3
Self-Serve	EventTracker-Support@Netsurion.com	1 (877) 333-1433 Option 1, Option 4

<https://www.netsurion.com/eventtracker-support>