



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	Ov	erview	4
	1.1	Uses of Application Control	4
	1.2	Application Control vs Anti-Virus	4
2	Ар	plication 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	Ар	plication Control Dashboard	8
	3.1	Groups Pane1	.1
	3.1	.1 Groups Overview	.2
	3.2	Pending Analyst Pane1	.3
	3.2	.1 Pending Analyst Overview	4
	3.3	Action Taken Processes Pane2	26
	3.3	.1 Action Taken Processes Overview 2	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
 Protects complete network and all its 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 malwares 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.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 II icon and click Application Control from the drop-down menu.





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

Se	nsors:	4								Overview
ups										Sensors
						Search	Gro	wp v Q	۹	ALERTING
-	-							•	Total	4
-								•	Total	NON REPORTING
-									Total	0
8.16									Total	
based	hate								Total	
-	-								Total	
(and									Total	
-									Total	
uge Siz	e 25	v c 1	of 1 GO	•						
ndine	a Anal	lyst Review:143				Search_	File Name	v Q	Ø	Overview
			-		-				-	143 Pending Processes
D	÷	File Found Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places 1	1	TERMINATED
0		0 minutes ago	manut	BINCING R	Photo America - Americana	Law	UNKNOWN	1	1	0
0	۲	0 minutes ago	graphites	BACING .	Photo American Street and Street	Low	UNKNOWN	1	1	NOT TERMINATED
	۲	2 minutes ago	100mg.d	BACKUR.	(*************************************	Low	UNKNOWN	1	ł	DORMANT
0	•	2 minutes ago	Terrenut me	BNCN/B	providements in electronic	Low	UNKNOWN	1	1	0
	(H)	2 minutes ago	Name Mondage	and the second	Private Association and Decision	Low	UNKNOWN	1	-	BULK ACTION
0		2 minutes ago	And the second s	BALLAN D	Photo America and American and	Low	UNKNOWN	1		Allow All
0	•	2 minutes ago	(Birep.d	BACK II	Photo Reserves to Alternative Re-	Low	UNKNOWN	1		Deny All
	÷	4 minutes ago	MOMODIA	BACK II	(Treasurers - ancouse	Low	UNKNOWN	2	I	
	۲	6 minutes ago	Birligh an	BNOV B	ETHERMOLE AND A RECOVER	Law	UNKNOWN	1	I	
0	•	6 minutes ago	dam.ca	BACIN'S	Photo Automation & Advancement	Low	SAFE	1	1	
0	(H)	6 minutes ago	And and an owned with the	and the second	Contraction of the local division of the loc	Low	UNKNOWN	1	1	
	•	6 minutes ago	Charlos and an and a second second	and the second	Provention - enclosed	Law	UNKNOWN	1	-	
0		6 minutes ago	Brian Process	BACK/R	STANDARD - ADDITION	Low	SAFE	2		
	۲	6 minutes ago	Bullinson	ancrea.	ETIME.NENT 1-ENCINCE	Low	UNKNOWN	1	1	
	ŧ	8 minutes ago	See georgeometer	BICOUR	ETHERAPITY & BROWN	Low	UNKNOWN	2	ł	
	•	8 minutes ago	100000 AM	BINCIN/ID	ETHNE REPORT FROM CONTR.	Law	UNKNOWN	1	1	
0	•	10 minutes ago	Landgebour di	BACIN'S	proved and the end of the	Low	UNKNOWN	1	1	
0		10 minutes ago	Autombule on	BALLAN D	17148-149111-8942918	Low	SAFE	1		
0	٠	10 minutes ago	analitie	BACK IN	17148-14911-1-89429418	Low	UNKNOWN	1	1	
	Ð	10 minutes ago	107-004 (%)	BALIN II	ETHNEJMENT - ADVCINUE	Low	UNKNOWN	1	I	
U	Ð	12 minutes ago				LOW	UNKNOWN	1		
ge Size	25	• < 1	of 6 GO	•						Quanting
tion	Taken	Processes: 1,147				Search	File Name	~ Q	۹	1217 Action Taken Prove
0		Action Taken Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places		Acknowledge A
	۲	6 minutes ago		BNCIN18	(The American Street and Street Barrier Street Barr	Low	SAFE	2	I	
0	•	Aug 30 05:28:21 PM	matha	Sectore	1100-0001	Serious	UNKNOWN	3	1	
0	(H)	Aug 30 05:28:21 PM	the later in an	Barrister.	COMPANY OF THE OWNER.	Serious	UNKNOWN	3	1	
0		Aug 30 05:06:22 PM	page and a second	BACING.	Print, Astron 1. Brillion	Low	UNKNOWN	1		
0	٠	Aug 30 05:06:22 PM		BINCING.	ETIME.NENT1 - ENCINE	Low	UNKNOWN	1	I	
	۲	Aug 30 05:06:22 PM	101102-0	for the last	and we	Serious	UNKNOWN	1	I	
	•	Aug 30 04:48:43 PM	Belgrand funderhal and	BINCING	production in and put	Law	UNKNOWN	1	ł	
0	•	Aug 30 04:42:22 PM	51.4	ancous	(True, Association and and and	Law	UNKNOWN	1	-	
		Aug 30 04:40:15 PM	and a	berlate.	10.00	Serious	UNKNOWN	1	-	
0	•	Aug 30 04:02:10 PM	mond	Sector.	810-001	Serious	UNKNOWN	1	1	
0	۲	Aug 30 03:56:23 PM	Second and second second	berhate	810.001	Serious	UNKNOWN	1	1	
	۲	Aug 30 03:52:24 PM	respiration of the second	BINCIPUS	ETHERAL AND CONTRACTOR	Low	UNKNOWN	1	I	
	•	Aug 30 03:38:18 PM	laster or the ter	BNCING	(*************************************	Low	UNKNOWN	1	I	
-	(H)	Aug 30 03:38:18 PM	Survey .	ancous	COMPANY'S CARACINAL	Low	UNKNOWN	1	;	
0		Aug 30 01:32:23 PM	information .	1000	NTOTALIST ACCURATE	High	UNKNOWN	1	;	
		Aug 30 10:52:11 AM	and the fit	BNCING.	(*************************************	Low	UNKNOWN	1	1	
	۲		Carlos a	ancoust.	ETHERAL CONTRACTOR	Low	UNKNOWN	1	1	
	•	Aug 30 09:54:15 AM	(RUNR) R		and the second s	Law	UNKNOWN	2		
	+ +	Aug 30 09:54:15 AM Aug 30 08:46:09 AM		BNCING.	provide states of the second					
	+	Aug 30 09:54:15 AM Aug 30 08:46:09 AM Aug 30 08:46:09 AM	and a	BACING BACING	Photo America and American	Low	UNKNOWN	2	1	
	+ +	Aug 30 09:54:15 AM Aug 30 08:46:09 AM Aug 30 08:46:09 AM Aug 30 08:46:09 AM	andtal andtal Inspiration or	BACINE BACINE BACINE	Producers 1 - and the	Law		2	1	
		Aug 30 09:54:15 AM Aug 30 08:46:09 AM	andra andra ingergennen inger	Brind Brind Brind Brind	11148-14411 - 414-144 11148-14441 - 414-144 11148-14441 - 414-144	Law Law Law		2 2 2	1	



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:

<u>Groups</u>

- **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.

ashboard	•	/ EventTracker / Application Control / Dasht
Total Sensors: 4		Overview
Groups		Sensors
	Search Group 🗸 🔍	ALERTING
BINCING	1 1 Total	4
875.	1 1 Total	NON REPORTING
BNDV3E	1 Total	0
ACMEDIE	1 1 Total	
Inethalar	1 1 Total	
ENCINE .	1 Total	
Default	0 Total	
Window	0 Total	
Page Size 25 V C 1 of 1 GO >		



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.

כ		File Found Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places		TERMINATED
	÷	0 minutes ago	System of Land	BINCINGS.	ETHERMOST FERRORISE	Low	UNKNOWN	1	1	0
	ŧ	0 minutes ago	ampro.dl	BINCINGS.	ETHNERARY I ADDRESS	Low	UNKNOWN	1	:	NOT TERMINATED
	ŧ	0 minutes ago	graphics and	BINCINGS.	ETHNERWIST FRICING	Low	UNKNOWN	1	:	1/12
	÷	2 minutes ago	(RONG-R	BINCINGS	ETHERAL HERE I AND NOT	Low	UNKNOWN	1	:	145
	÷	2 minutes ago	Terrenutione	BINCINGS.	(TWARRANT) 1-BINCINGS	Low	UNKNOWN	1	:	DORMANT
	÷	2 minutes ago	Index Mindage	BINCIN'S	ETHERAL HARD I AND NO.	Low	UNKNOWN	1	:	U
	+	2 minutes ago	Ingeniese	BINCIN'S	(TMR/MINT) 1-BNCN/3E	Low	SAFE	1	:	BULK ACTION
	+	2 minutes ago	Restandant and	BINCINGS.	ETHERMOST I ANONIS	Low	UNKNOWN	1	:	Allow All
	+	2 minutes ago	(Ringel	BINCINGS.	(TARGER 11 - RECOVER	Low	UNKNOWN	1	:	Deny All
	+	4 minutes ago	MORIDA.	BINCINGS.	ETHERAL AND LANCING	Low	UNKNOWN	2	:	
	÷	6 minutes ago	whitphase	BINCING.	(TMB/MRT11-BNCN18	Low	UNKNOWN	1	:	
	÷	6 minutes ago	part and	BINCINGS.	ETHNELINENT I ANONIS	Low	SAFE	1	:	
	÷	6 minutes ago	autodyne	BINCING.	(TABLARY) I-BNOV II	Low	UNKNOWN	1	1	
	÷	6 minutes ago	Delosterenhophs.#	BINCIN'S	ETHERARY I AND NO.	Low	UNKNOWN	1	;	
	÷	6 minutes ago	Sherease	BINCIPUID.	ETHNERAL I ANCHOR	Low	UNKNOWN	1	:	
	÷	6 minutes ago	design and and	BINCOV IS	ETHERAL HANCE & ADDRESS	Low	SAFE	2	:	
	+	6 minutes ago	Bulliotae	BINCING B	ETHERAL HENCING	Low	UNKNOWN	1	1	
	+	8 minutes ago	Grouper prints and	BINCING 8	ETHNEJMENT I AND/OUT	Low	UNKNOWN	2	:	
	+	8 minutes ago	\$2200.00	BINCINGS.	ETHNEJMENT I BINCHUR	Low	UNKNOWN	1	:	
	÷	10 minutes ago	UneMpProp.8	BINCINGS	ETHERARY I ADDITION	Low	UNKNOWN	1	1	
	÷	10 minutes ago	accelded.	BINCING R	ETHERMOLI I BINCHUR	Low	UNKNOWN	1	:	
	+	10 minutes ago	Rationalisate and	RINCOV D	ETHALIANCI I ANONIS	Low	SAFE	1	:	
	÷	10 minutes ago	anadri.dl	BINCING.	ETHERMOST 1-RECOVER	Low	UNKNOWN	1	:	
	÷	10 minutes ago	UNTHENEDIA	BINCING B	ETHNEJAMOT I - RINCOVIN	Low	UNKNOWN	1	;	
	÷	12 minutes ago	Printed and	BINCING R	ETHERMOLT I BOOM IN	Low	UNKNOWN	1	:	



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.

							10	-	1217 Action Taken Processes
C	Action Taken Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places		Acknowledge All
) 🕀	6 minutes ago	4010070.00	BNOV H	ETHERMONY FANCING	Low	SAFE	2	:	Acknowledge Air
•	Aug 30 05:28:21 PM	acadituli	berthaler	8155-WH	Serious	UNKNOWN	3	:	
) 🕀	Aug 30 05:28:21 PM	man	bertfacter	Account.	Serious	UNKNOWN	3	:	
) 🕀	Aug 30 05:06:22 PM	Not Springforces	RNON8	(TMURROWS I HANCOUR	Low	UNKNOWN	2	:	
) 🕀	Aug 30 05:06:22 PM	physical and the second s	RNCNH	(TMB/MN111-BNCNIE	Low	UNKNOWN	1	:	
) 🕀	Aug 30 05:06:22 PM	acudit.M	RNCN0	UTMERMONT I ADDING	Low	UNKNOWN	1	:	
•	Aug 30 05:06:22 PM	(Ringat	for Cale	8153-9841	Serious	UNKNOWN	1	:	
) 🕀	Aug 30 04:48:43 PM	Relignant/Inschritist.exe	BNCN/F	ETHABLEMENTS I - MINICIPALE	Low	UNKNOWN	1	:	
) (†	Aug 30 04:42:22 PM	30.4	BNCNH	ETHNEJIMMUS I ANCINE	Low	UNKNOWN	1	:	
) 🕀	Aug 30 04:40:15 PM	analitat	BNCN/E	ETHERMOLI - ENCINE	Low	UNKNOWN	1	:	
) 🕀	Aug 30 04:28:32 PM	acaddud	Eventhadar.	8103-WH	Serious	UNKNOWN	1	:	
) (†	Aug 30 04:02:10 PM	record.	for the last	RID WE	Serious	UNKNOWN	1	:	
) +	Aug 30 03:56:23 PM	System Settings Adminificant and	Event Tracher	R103-0441	Serious	UNKNOWN	1	:	
•	Aug 30 03:52:24 PM	respirate to the second	RNONR .	UTVMEARN111-BINCING	Low	UNKNOWN	1	:	
•	Aug 30 03:38:18 PM	SpolitConOlg.law	BNCN0	ETHERMOLI I ANCINE	Low	UNKNOWN	1	:	
•	Aug 30 03:38:18 PM	Silling.	BNCN0	(TMB/MN111-BNCN0)	Low	UNKNOWN	1	:	
) 🕀	Aug 30 01:32:23 PM	SpectrituleCoartial are	#NCNO	ETHERAL HENCING	Low	SAFE	1	:	
•	Aug 30 01:20:16 PM	configmentages 2.48	ADDE	NPUTRATE-ACHEOR	High	UNKNOWN	1	:	
) 🕀	Aug 30 10:52:11 AM	analitati	RNONH .	ETHNERWICH I ADDODG	Low	UNKNOWN	1	:	
) 🕀	Aug 30 09:54:15 AM	(Ring-R	ancrea	UTVMEARN111-RENCINE	Low	UNKNOWN	1	:	
) 🕀	Aug 30 08:46:09 AM	and A.B.	RNONE .	ETIMERAN'S FANCING	Low	UNKNOWN	2	;	
) 🕀	Aug 30 08:46:09 AM	analist.	RNCN/F	ETTAMENANCI I - BINCING	Low	UNKNOWN	2	:	
) 🕀	Aug 30 08:46:09 AM	(impletation on	RINCING.	(TMEANN'S FRICING	Low	UNKNOWN	2	:	
) 🕀	Aug 30 08:46:09 AM	scape.dl	RNONH .	ETHERMORY 1-RINCING	Low	UNKNOWN	2	:	
) 🕀	Aug 30 08:12:17 AM	ametric) (CL	ADDE	NPUTRAIN-ADMIN	High	UNKNOWN	1	:	



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.

Groups			
	Search	Group	ର୍ ଷ୍
Default		Sensor	4 🕢 4 Total
EventTracker		•	🚺 🚺 1 Total
NTPL		•	1 Total
PRISM		•	1 Total

• Each color indicates a Group status.

Groups			Sensors	
	Search Group	~ Q, Q,	ALERTING	0
	r	• 2 Tabel	11	
		1 2 lotal		
Eh imt fact in Groups	Status	1 Total	NON REPORTING	
W.ED. ESC. VY		1 Total	3	

• 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.

PRISMSYS	Group			1 2 Total
CONTACT NAME	CONTACT PHONE	CONTACT EMAIL		
R 54-\ VI3~Pr	i 1sys - Win 8.1		Process status of the	000
N PLD I LR30	ris sys-Win 10	Sensors	sensors	



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

Color	Status	Description
Orange 0	DORMANT	Indicates the number of files detected before execution.
Red 🧿	TERMINATED	Indicates the Terminated process by the Netsurion Application Control.
Fountain Blue 0	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.

PRISMSYS	1 2 Total
CONTACT NAME CONTACT PHONE CONTACT EMAIL	
K 154-VIVI5~PTISHISYS - WIII 0.1	000
NTTL DTDL D20. D-1 145- 10	0 0 0 NR

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).

Dashboard	♠ / EventTracker / Application Control / Dashboa
Dashboard Total Sensors: 4 Groups Group Group Q Group	 A / EventTracker / Application Control / Dashboa Overview Sensors ALERTING ALERTING
MINCONDE 11 Defeat 01	otal
0 T	otal

Color	Status	Description			
Yellow 1	ALERTING	This status shows all the locations or systems where a new process has appeared.			
Gray 1	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.

Total Sensors: 5		Overview
Alerting × Clear All ×		Sensors
Groups		ALERTING
	Search Group 🗸 🔍	5
RNDOI	1 Total	NON REPORTING
879,	1 1 Total	0
BNDV/B	1 1 Total	
Lectule	1 1 Total	
ACMERT	1 1 Total	

• **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.

Dashboard				A	/ EventTracker / Application Control / Dashbox
Total Sensors: 5					Overview
NonReporting 🗙 Clear All 🗙					Sensors
Groups					ALERTING
	Search_	Group 🗸	ର୍ ୧	۲	5
BNCNB			1 Tot	1l	NON REPORTING
					0

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.

Pendin	g Anal	lyst Review:10,68	7		Search		File Name Sensor Name	Q	Q
		File Found Time	File Name	Location Name	Sensor	Asset Value	Hash Location		
	+	a minute ago	dosvc.dll	AI SH	N' PLE "B' 724~# IIME5 H	Low	Opinion Product Name		1
	(+)	a minute ago	d rc ill	Al SH	Nº PLE "B 324~# IIMES 1	Low	Signed By File Path		÷
	(+)	2 minutes ago	n (d. sys	AI 5H	Nº PLE "BI \$24~# IIMES 1	Low	Parent Process Path		÷
	(+)	2 minutes ago	w pc .dll	AI 5H	Nº PLE "B 324~# IIMES 1	Low	UNKNOWN 1		
	(+)	4 minutes ago	ui bt 1.dll	AI SH	N° PLE 'B 324~# IIMES 1	Low	UNKNOWN 2		÷
	$\left(+\right)$	6 minutes ago	A ɔ_' ؛b_oa25k2ei.dll	L H M	ET VN 3L 22012 3~m; hili	High	UNKNOWN 1		÷

- 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.

	File Found Time	File Name		Location Name	Sens	or			Asset Value	Opinion	Allow	
ŧ	0 minutes ago	dosvc.dll		' EDN"SDAY	ΝPI	LDT-	R30~V`edn	day	Low		Deny	
+	6 minutes ago	NTL INMA	.DLL	, VIME (H	N PI	LDT	R24~# NIMI	н	Low		Research	
+	6 minutes ago	drp ov.dll		, NIME (H	ΝPI	LDT	R24~# NIMI	н	Low	UNKNOWN	1	_
+	7 minutes ago	mrx lav.sys		, vime (H	N PI	LDT	R24~# NIMI	н	Low	UNKNOWN	1	
+	7 minutes ago	wet :Int.dl		, vime H	ΝPI	LDT	R24~# VIMI	н	Low	UNKNOWN	1	
÷	9 minutes ago	uirit bon.d		, vime H	N PI	LDT	R24~# NIMI	н	Low	UNKNOWN	2	
+	11 minutes ago	Apr Web	a25k2ei.dll	I YTHI J	ΕΓV	/ME	₹22012 3~n	thili	High	UNKNOWN	1	
÷	11 minutes ago	Apr Web	/kmiqh.dll	I YTHI J	ΕΓV	/ME	₹22012 3~n	thili	High	UNKNOWN	1	
+	11 minutes ago	msj toledt	0.dll	I YTHI J	ΕΓV	/ME	₹22012 3~n	thili	High	UNKNOWN	3	
ŧ	11 minutes ago	QUI RY.DLI		, vime H	N PI	LDT	R24~# VIMI	н	Low	SAFE	2	
(+)	12 minutes ago	Apr Web	1puo2et.dll	L.YTHI J	ΕΓV	/ME	₹22012 3~n	thili	High	UNKNOWN	1	

Allowing the process

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

Allow Process				×
File Name: Signed by:	dosvc.dll N/A	Opinion:	UNKNOWN	
	Global 🕲		Select Group	
add comments here.	**			
				Allow Close

- 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.

Allow Process				×
File Name: Signed by:	dosvc.dll N/A	Opinion	UNKNOWN	
	Global 🕲		Select Gro	up 9
add comments here.	**			
				Allow Close



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

rile Name:	dosvedii	
Signed by:	N/A	Opinion: UNKNOWN
	Global 🐼	Select Group 9
ailable Groups		Selected Groups
Win 7 and Server Win XP and Server Domain Controlle Firewall Devices Network Devices VmWare A28 After Dark After Dark After Dark After Dark After Dark Arter and After Dark Arter and Arter and Arsenal BangaloreCentral Barcelona	2003 Above ir 2003 ers	
d comments here		

Denying the process

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

c	Deny Process X								
	File Name: Signed by:	dosvc.dll N/A	Opinion:	UNKNOWN					
		Global 🔕		Select Group 9					
	add comments here								
				Deny	se				



- 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.

•	Deny Process				×
	File Name: Signed by:	dosvc.dll N/A	Opin	ion: UNKNOW	N
		Global 🕲		Selec	t Group 9
	add comments here	Global 🕲		Selec	t Group 🛛

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

Deny Process				×
File Name: Signed by:	dosvc.dll N/A	Opinion:	UNKNOWN	
Available Groups	Global 🕲		Select Group	
Allensolly AmericanExpress Armani Arsenal BangaloreCentral Barcelona BeingHuman BigBazar Blackberry Blenders Pride BrandFactory Burberry Carvir-ESP Carvir-USA				~
add comments here				
				Deny Close



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.

nding	g Anal	yst Review:10,68	3					Search		File Nam
		File Found Time	File Name		Location Name	Senso	,		Asset Value	Opinion
	\pm	0 minutes ago	dosvc.dll		' EDN ⁻ SDAY	N PLC	T .R30~V`edr	⊨ day	Low	UNKNOW
	\pm	6 minutes ago	NTL ANMA	.DLL	JIME H	N PLC	T .R24~# NIM	н	Low	UNKNOW
	\pm	6 minutes ago	drp əv.dll		, JIME H	N PLC	T .R24~/ NIN	н	Low	UNKNOW
	(\pm)	7 minutes ago	mrx lav.sys		JIME H	N PLC	R24~# NIN	н	Low	UNKNOW
	\pm	7 minutes ago	wet :Int.dl		, JIME H	N PLC	T .R24~# NIN	н	Low	UNKNOW
	\pm	9 minutes ago	uirit bon.d		, vime sh	N PLC	T .R24~/ NIM	ы	Low	UNKNOW
	\pm	11 minutes ago	Apr Web_	a25k2ei.dll	I YTHI J	E IVN	IE 322012 3~	n thili	High	UNKNOW
	\pm	11 minutes ago	Apr Web_	/kmiqh.dll	L YTHLI	E IVN	IE 322012 3~1	n thili	High	UNKNOW
	+	11 minutes ago	msj toledt	0.dll	I YTHI I	ETVN	IE 322012 3~	n thili	High	UNKNOW
	+	11 minutes ago	QUI RY.DLI		, vime (H	N PLC	r .R24~# NIM	ы	Low	SAFE
	+	12 minutes ago	Apr Web_	ipuo2et.dll		E IVN	IE 322012 3~I	n thili	High	UNKNOW

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

1 File Names le Version 10.0		CTTTTTDE CTTTO-E					1	
oduct Name Mic).17763.1 rosoft® Windows® Ope	rating System	Q	ETTVMBLR2W10-2 ETTVMBLR22019-4	6 hou Aug 17 06:23 PM	urs ago 3.44	2	115 NOT TERMINATED 9,089
ounter Signed By N/A								DORMANT 12,358
e Modified Time Sep arent Process Name SVCP	01 07:57:18 AM host.exe	Allow	Deny					BULK ACTION
arent Process Path C:\V	Windows\System32\svch	ost.exe)eny					Deny All
arent Process Hash 23e4	47ce30cfc49f60a6e24b50	sa83b9b						
arran Gal		Allow	Deny					
	ned By N/A ned On · · · · · · · · · · · · · · · · · ·	ned By N/A	ned By unter Signed By N/A ned On Modified Time Sep 01 07:57:18 AM ent Process Name Svchost.exe Allow C:\Windows\System32\svchost.exe Allow C:\Windows\System32\svchost.exe Allow C:\Windows\system32\dstokenclean.exe Allow C:\Windows\system32	ned By VIA Unter Signed By N/A Unter Signed By N/A ned On Modified Time Sep 01 07:57:18 AM ent Process Name svchost.exe Allow Deny ent Process Path C:\Windows\System32\svchost.exe Allow Deny ent Process Hauh 23e47ce30cfc49f60a6e24b50aa83b9b ent Process Hauh 23e47ce30cfc49f60a6e24b50aa83b9b ent Process Hauh 23e47ce30cfc49f60a6e24b50aa83b9b ent Brocess Hauh 23e47ce30cfc49f60a6e24b50aa83b9b ent Brocess Hauh 23e47ce30cfc49f60a6e24b50aa83b9b ent Process Hauh 23e47ce30cfc49f60a6e24b50aa83b9b ent Brocess Hauh 24e47ce30cfc49f60a6e24b50aa83b9b ent	ned By Unter Signed By N/A unter Signed By N/A ned On Modified Time Sep 01 07:57:18 AM ent Process Name SvChost.exe Allow Deny ent Process Hash 23e47ce30cfc49f60a6e24b50ae33b9b ent Process Hash 23e47ce30cfc49f60a6e24b50ae33b9b ent Process Hash 23e47ce30cfc49f60a6e24b50ae33b9b ent Process Hash 23e47ce30cfc49f60a6e24b50ae3b9b ent Process Hash 23e47ce30cfc49f60afe24b50ae3b9b ent Process Hash 24b60f7c10ce0	ned By ETTWIDLR22(1):9-4-09 Tricks BM Bolt PM BoltR22(1):9-4-09 Tricks BM BoltR22(1):9-4-09 Tricks	ned By LITINDER22019-4003 IT INCLUS	ned By Unter Signed By N/A PM



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

🗌 😑 6 hours ago dstokenclear	n.exe	NTPL ETTVMBLR2W10-2 L	ow	SAFE 2	÷	21,401 Pending Processes
Thans 400606	1 Fie Names			Detected on sensors	2	115
IP Address 172.28.9.164	File Version	10.0.17763.1	-	ETTVMBLR2W10-2 6 hours ago		NOT TERMINATED
Log Time Computer Sep 01 07:57:18 AM ETTVMBLR2W10-2	Product Name Signed By	Microsoft® Windows® Operating System	Ц	ETTVMBLR22019-4Aug 17 06:23:44 PM		9,089
Contact	Counter Signed By	N/A				DORMANT
1	Signed On					12,358
Launched by:	File Modified Time	Sep 01 07:57:18 AM				BULK ACTION
Domain User Name NT AUTHORITY SYSTEM	Parent Process Name	svchost.exe	0			Allow All
Observation Process does not match the allowed process criteria.	Parent Process Path	C:\Windows\System32\svchost.exe) 🗋			Deny All
	Parent Process Hash	23e47ce30cfc49f60a6e24b50aa83b9b				
	File Path	C:\Windows\system32\dstokenclean.exe)[]			
	Hath	6a7d3561hcha33ed64e3hefd67c10ca0				

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.

ding Analyst Review:12,589	Searc	h File Name 🖌 Q, Q,	Overview
I hours App_Web_jzh5vxid.c ago	II EventTracker ETTVMBLR22019-4	Serious UNKNOWN 1	12,589 Pending Processes
Thane, 400606 IP Address 172,28,9,147 Log Time Computer Sep 04 10:30,54 AM ETTV/MBLR22019-4 Contract Employed	1 Fie Names Fie Version 0.0.0.0 Product Name Signed By Counter Signed By N/A Signed On	Detected on sensors 1 ETTVIMBLR22019-4 1 hours ago	93 NOT TERMINATED 251 DORMANT 12,250
Launched by: Domain User Name NT AUTHORITY NETWORK SERVICE	File Modified Time Sep 04 10:30:54 AM Parent Process Name w3wp.exe Allow Deny		BULK ACTION Allow All
Observation Process loaded a binary that does not	Parent Process Path C:\Windows\SysWOW64\inetsrv\w3wp.exe Allow Deny		Ueny All



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

Select Group 💡
Add Clo

- 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.

D 1 hours ago NTC	exe	EventTracker	ETTVMBLR22019-1	Serious	UNSAFE	1 :
Gurgaon, 122002 IP Address 172.28.9 Log Time Computer Feb 01 08:10:56 PM ETTVMBLR22019-1 Contact	4 1 File Names File Version Product Name Signed By	0.7 SLEEP		Q	Detected on sensors ETTVMBLR22019-1	1 1 hours ago
E	Counter Signed By Signed On	N/A				
Launched by:	File Modified Time	Feb 01 08:10	0:56 PM			
NTPL prathik.g	Parent Process Nam	e explorer.exe		Allow Deny		
Observation	Decent Decence Deth	CiWindowd				
Process does not match the allowed process criteria.	Parent Process Path	C.\Windows	explorer.exe	Allow Deny		
	Parent Process Hasi	c6cd12bf63e	e9b9b4478e6f975e7c293d			
	File Path	C:\Users\pra	thik.g\Desktop\NTC7.exe	Allow Deny		
	Hash	2fc019e71a9	817a96430bd24ce360ab2 Allov	v Deny Research		
	Hash Opinion UNSAFE Opinion Link Threat Center F	Opinion Reference Netsurion Thre	e Opinion Ratio at Center 2/39 Threat En	Risk Threshold 2 gine: IBM XFE Team Cymru		



- 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.

If the Hash is found unsafe in the Netsurion Threat Center, then the Hash opinion is provided as UNSAFE. 0 0 1 hours ago NTC7.exe ETTVMBLR22019-1 : EventTracker Serious UNSAFE Detected on sensors 1 File Name 1 Gurgaon, 122002 IP Address 0.7 File Version 172.28.9.4 ETTVMBLR22019-1 1 hours ago SLEEP Product Name Log Time Computer Feb 01 08:10:56 PM ETTVMBLR22019-1 Signed By Contact Counter Signed By N/A 12 Signed On Launched by: Feb 01 08:10:56 PM File Modified Time User Name prathik.g **Hash Opinion** Domain NTPL Parent Process Name explorer.exe Allow Deny Observation UNSAFE Parent Process Path C:\Windows\explorer.exe Process does not match the allowed process criteria. Allow Deny c6cd12bf63e9b9b4478e6f975e7c293d Parent Process Hash C:\Users\prathik.g\Desktop\NTC7.exe File Path Allow Deny Hash 2fc019e71a9817a96430bd24ce360ab2 Allow Deny Research Hash Opinion Risk Threshold Opinion Reference Opinion Ratio UNSAFE Netsurion Threat Center 2/39 2 Threat Engine: IBM XEE Team Cymru Threat Center Feed The Hash opinion is specified as UNKNOWN if the Hash is not available in the **Hash Opinion** Netsurion Threat Center, is neither found to be UNSAFE nor below the Threshold UNKNOWN value, and a lookup from Virus Total is not possible.

The Netsurion Threat Center provides the following Opinions.



		1 File Names			Detected on sensors	
Gurgaon, 122002	172 28 9 4	File Version	1.8		ETTV/MPI 000010_1	a minut
Log Time Comput	lar land	Product Name	SLEEPIA		ETTVMBLK22019-1	a minut
Feb 01 06:07:50 PM ETTVM	BLR22019-1	Signed By				
Contact		Counter Signed By	N/A			
		Signed On				
Launched by:		File Modified Time	Feb 01 06:07:50 PM			
NTPL Domain User Nar prathik.	.g	Parent Process Name	explorer.exe			
Observation				Allow Deny		
Process does not match the al criteria.	lowed process	Parent Process Path	C:\Windows\explorer.exe	Allow Deny		
		Parent Process Hash	c6cd12bf63e9b9b4478e6f975e7c293d			
		File Path	C:\Users\prathik.g\Desktop\NTC18.exe	Allow Deny		
		Hash	bacc54cbedff0173d0fafda27d09680a Allow D	eny Research		
		Hash Opinion Opin UNKNOWN Nets	ion Reference Opinion Ratio Risk Thre surion Threat Center 0/0 1	shold Opinion Link		
		Threat Engine: IBM X	FE Team Cymru			

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

D 1 hours ago NTC7.exe		EventTracker	ETTVMBLR22019-1	Serious	UNSAFE	1	:
Curran 122002	1 File Names				Detected on sensors		1
IP Address 172.28.9.4	File Version	0.7			ETTVMBLR22019-1	1 hours ago	
Log Time Computer Feb 01 08:10:56 PM ETTVMBLR22019-1	Signed By	SLEEP					
Contact	Counter Signed By	N/A					
	Signed On						
Launched by:	File Modified Time	Feb 01 08:10:5	6 PM				
NTPL prathik.g	Parent Process Name	explorer.exe					
Observation				Allow [Delly]			
Process does not match the allowed process criteria.	Parent Process Path	C:\Windows\e	xplorer.exe	Allow Deny			
	Parent Process Hash	c6cd12bf63e9	b9b4478e6f975e7c293d				
	File Path	C:\Users\prath	ik.g\Desktop\NTC7.exe	Allow Deny			
	Hash	2fc019e71a98	17a96430bd24ce360ab2 Allo	w Deny Research			
	Hash Opinion UNSAFE Opinion Link	Opinion Reference Netsurion Threat	Opinion Ratio Center 2/39 Threat Er	Risk Threshold 2 Igine: I <u>BM XFE Team Cymru</u>			

Threat Center Feed Source Details

1 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.

D 1 hours ago NTC7.exe		EventTracker	ETTVMBLR22019-1	Serious	UNSAFE	1 :
Gurgaon, 122002 IP Address 172.28.9.4 Log Time Computer Feb 01 08:10:56 PM ETTVMBLR22019-1 Contact	1 File Names File Version Product Name Signed By Counter Signed By	0.7 SLEEP N/A		D	Detected on sensors	1 1 hours ago
Launched by: Domain User Name NTPL prathik.g	Signed On File Modified Time Parent Process Name	Feb 01 08:10:56 PM explorer.exe		Allow Deny		
Observation Process does not match the allowed process criteria.	Parent Process Path	C:\Windows\explore	er.exe	Allow Deny		
	File Path	C:\Users\prathik.g\[Desktop\NTC7.exe	Allow Deny		
	Hash Hash Opinion UNSAFE Opinion Link	2fc019e71a9817a96 Opinion Reference Netsurion Threat Cent	430bd24ce360ab2 Allow Opinion Ratio er 2/39 Threat Engl	Deny Research Risk Threshold 2 ine: IBM XFE Team Cymru		

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.

	25 minutes ago Vaccine3.exe		EventTracker	ETTVMBLR22019-	1 Se	rious	UNSAFE	1	
Hash Opinion UNSAFE	Gurgaon, 122002 IP Address 172.28.9.4 Log Time Computer Feb 01 06:19:51 PM ETTVMBLR22019-1 Contac User Name NS5 PK5 Observation Process does not match the allowed process criteria.	1 File Names File Version File Version File Version Foduct Name Signed By Signed Dy Counter Signed By Signed On File Modified Time Parent Process Path Parent Process Path File Path File Path Hash Copinion Ink https://www.inustota KachdsSeeD11c/detect 4fab3/dreefbb/004a7111 Threat Engine: IBMX	0.6 SLP01 N/A Feb 01 06:19:51 PM explorer.exe C:\Windows\explorer.ex f070b5ct25febb9a88a16 C:\Users\prathik.g\Desk b1563f567dd1922t27f7/ Opinion Reference VirusTotal Lcom/gui/file/4fab9dfe6fbb ion/f: 7/d Te3e705f06252c18d7d3 EE Team.Cymru	e s8efd87c6112 top\Vaccine3.exe d0b300c27d2b Allc 50bfa7f1f7d1e3e705 3fd6b7cf618cbdb56	Allow Deny Allow Deny Allow Deny Allow Deny Mu Deny Research Copinion Ratio 42/56 copinion Ratio 42/56 copinion Ratio		Vetected on sensors	25 minutes ago	
Hash Opinion	Hash found safe from	Virus Tot	al.						



		1 File Names				Detected on sensors	s	
	IP Address 172.20	File Version	10.0.17763.1			ETTVMBLR22019-1	14 mi	inutes ago
	Log Time Computer	Product Name	Microsoft® Windows® Operatin	g System				
	Feb 20 12:55:47 PM ETTVMBLR22019-1	Signed By						
	Contact	Counter Signed By	N/A					
		Signed On						
	Launched by:	File Modified Time	Feb 20 12:55:47 PM					
	Domain User Name NT AUTHORITY SYSTEM	Parent Process Name	net.exe			1		
		-						
	Observation Process does not match the allowed process	Parent Process Path	C:\Windows\SysWOW64\net.exe			1		
	criteria.				Allow Deny L	1		
		Parent Process Hash	cb0744aa7acb8b8a960fcce32597	'39ec				
		File Path	C:\Windows\SysWOW64\net1.ex	e				
					Allow Deny]		
		Hash	e28124dt01ca/9td93t3b/c48deo	dad0 Allow Deny	Research			
		Hash Opinion	Opinion Reference	Opi	inion Ratio			
		SAFE	VirusTotal	0/6	59			
		Opinion Link https://www.virustotal	.com/gui/file/383ecc5dbcdd98163c556	5ca6e4486c5dc6a3	5c3f1cff88dcf12da2cdaba80	19		
		70/detection/f-383eo	:5dbcdd98163c556ca6e4486c5dc6a35c	3f1cff88dcf12da2o	daba80970-1675690895			
		Inreat Engine: IBM X	FE Team Cymru					
	Hash found unkno	wn from Vi	rus Total					
	Hash found unkno	wn from Vi	rus Total.					
	Hash found unkno	wn from Vi	rus Total.	ETTVMBLR22019	9-1	Serious UNKNC	DWN 1	
	Hash found unkno	wn from Vi C17.exe	rus Total. Eventīracker	ETTVMBLR22015	9-1	Serious UNKNC Detected on see	DWN 1 nsors	
	Hash found unkno	WN from Vi C17.exe 1 File Names File Version	rus Total. EventTracker 1.7	ETTVMBLR22019	9-1	Serious UNKNC Detected on see ETTVMBLR220	DWN 1 Insors	minute aqu
	Hash found unkno	Wn from Vi C17.exe 1 File Names File Version Product Name	rus Total. Eventīracker 1.7 SLEEPIA	ETTVMBLR22019	9-1	Serious UNKNC	DWN 1 nsors 019-1 au	minute ag
	Hash found unkno	wn from Vi C17.exe 1 File Names File Version Product Name 1 Signed By	rus Total. EventTracker 1.7 SLEEPIA	ETTVMBLR22015	9-1	Serious UNKNC Detected on set ETTVMBLR220	DWN 1 nsors D19-1 au	minute ag
	Hash found unkno	wn from Vi C17.exe 1 File Names File Version File Version Signed By Counter Signed By	rus Total. Eventīracker	ETTVMBLR22015)-1	Serious UNKNC Detected on see ETTVMBLR220	DWN 1 nsors D19-1 ai	minute ag
	Hash found unkno	wn from Vi C17.exe 8.9.4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	rus Total. EventTracker	ETTVMBLR22015	9-1	Serious UNKNC Detected on see ETTVMBLR220	DWN 1 nsors D19-1 a i	minute ag
	Hash found unkno	wn from Vi C17.exe R9.4 1 1 Counter Signed By Counter Signed By Co	rus Total. EventTracker	ETTVMBLR22015	9-1	Serious UNKNC Detected on set ETTVMBLR220	DWN 1 nsors D19-1 au	minute age
ash	Hash found unkno	wn from Vi C17.exe 8.9.4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	rus Total. EventTracker	ETTVMBLR22015	9-1	Serious UNKNC	DWN 1 nsors D19-1 an	minute age
ash	Hash found unkno	WIN FROM Vi C17.exe 8.9.4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	rus Total. EventTracker	ETTVMBLR22015	9-1	Serious UNKNC Detected on see ETTVMBLR22C	DWN 1 nsors D19-1 a I	minute age
ash	Hash found unknoo	Wn from Vi C17.exe 8.9.4 1 1 Curter Signed By Signed On File Mames File Mames Signed On File Mames Parent Process Name	rus Total. EventTracker	ETTVMBLR22015	9-1 [Serious UNKNC Detected on ser ETTVMBLR22C	DWN 1 nsors D19-1 a I	minute age
lash inion NOWN	Hash found unkno	wn from Vi C17.exe 8.9.4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	EventTracker EventTracker 1.7 SLEEPIA N/A Feb 01 04:46:58 PM explorer.exe C:\Windows\explorer.exe	ETTVMBLR22015	9-1 [Allow (Deny) [Allow (Deny]	Serious UNKNC Detected on ser ETTVMBLR22C	DWN 1 nsors D19-1 ai	minute age
lash inion NOWN	Hash found unkno a minute ago NT Gurgaon, 122002 IP Address 172.2 Log Time Feb 01 04-46-58 PM Contact Computer Feb 01 04-46-58 PM Contact Launched by: Domain User Name NTPL prathik.g Observation Process does not match the allowed proc criteria.	wn from Vi C17.exe 8.9.4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	EventTracker EventTracker 1.7 SLEEPIA N/A Feb 01 04:46:58 PM explorer.exe C:\Windows\explorer.exe c6cd12b/63e9b9b4478e6/9	ETTVMBLR22015	9-1 [Allow] (Deny) [(Allow) (Deny) [Serious UNKNC Detected on set ETTVMBLR220	DWN 1 Insors D19-1 au	minute ago
ash inion NOWN	Hash found unkno	wn from Vi C17.exe 8.9.4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	rus Total. EventTracker 1.7 SLEEPIA N/A Peb 01 04:46:58 PM explorer.exe C:\Windows\explorer.exe C:\Windows\explorer.exe C:\Windows\explorer.exe c6cd12bf63e9b9b4478e6f9 C.\Users\prathik.g\Desktop	ETTVMBLR22015	3-1 [Allow] (Deny) [(Allow) (Deny) [Serious UNKNC	DWN 1 Insors 219-1 au	minute ag
ash inion NOWN	Hash found unkno	wn from Vi C17.exe 8.9.4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Fus Total. EventTracker 1.7 SLEEPIA N/A Feb 01 04:46:58 PM explorer.exe C:\Windows\explorer.exe c6cd12bf63e9b9b4478e6f9 C:\Users\prathik.g\Desktop	ETTVMBLR22015	9-1 Allow (Deny) [Allow (Deny) [Serious UNKNC Detected on set ETTVMBLR22C	DWN 1 nsors D19-1 a	minute ag
lash inion NOWN	Hash found unkno	wn from Vi C17.exe 8.9.4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Fus Total. EventTracker 1.7 SLEEPIA N/A Feb 01 04:46:58 PM explorer.exe C:\Windows\explorer.exe c6cd12b/63:e9b9b4478e6f9 C:\Users\prathik.g\Desktop d7e188t/6db/8b66ffddz38aa	ETTVMBLR22015 75e7c293d 17030fb2 Allow	3-1 Allow Deny [Allow Deny] Allow Deny [Deny Research]	Serious UNKNC Detected on set ETTVMBLR220	DWN 1 nsors D19-1 ai	minute age
lash iinion NOWN	Hash found unkno	wn from Vi C17.exe 8.9.4 1	EventTracker EventTracker 1.7 SLEEPIA N/A explorer.exe C:\Windows\explorer.exe C:\Windows\explorer.exe C:\Uindows\explorer.exe C:\Uindows\explorer.exe C:\Uindows\explorer.exe C:\Uindows\explorer.exe d:Te188ff6db/8b66ffd4238a d:Te188ff6db/8b66ffd4238a	ETTVMBLR22015	P-1 Allow (Deny) Allow (Deny) Allow (Deny) Deny Research	Serious UNKNC Detected on see ETTVMBLR220	DWN 1 Insors D19-1 au	minute age
ash inion NOWN	Hash found unkno	wn from Vi C17.exe 8.3.4 1	Fus Total. EventTracker 1.7 SLEEPIA N/A explorer.exe C:\Windows\explorer.exe C:\Windows\explorer.exe c6cd12bf63e9b9b4478e6f9 C:\Users\prathik.g\Desktop d7e188ff6dbf8b66ff64238a Opinion Reference Opinion Reference Opinion Reference Opinion Reference	ETTVMBLR22015 75e7c293d 172030fb2 Allow	2-1 (Allow Deny [Allow Deny [Allow Deny [Allow Deny [Deny Research]] Opinion Link www.virustotal.com	Serious UNKNC	DWN 1 nsors D19-1 at	minute age



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**.

Pendir	a Analys	t Review-840			Court		51 A		0 0	Overview	
i crian	grananja				Search		File Name	Ŷ	4 4	840 Pending Processes	
		File Found Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places		TERMINATED	0
	+	11 minutes ago	sppc.dll	EventTracker	R1S5-VM6	Serious	SAFE	1	1	0	
	+	12 minutes ago	SLC.dll	EventTracker	R1S5-VM6	Serious	SAFE	1	1	NOT TERMINATED	
	+	13 minutes ago	uxinit.dll	EventTracker	R1S5-VM6	Serious	SAFE	1	1	910	Ŭ
	+	13 minutes ago	kbdus.dll	EventTracker	R1S5-VM6	Serious	SAFE	1	1	010	
	+	13 minutes ago	SXS.DLL	EventTracker	R155-VM6	Serious	SAFE	1	1	DORMANT	0
	+	17 minutes ago	ploptin.dll	WEDNESDAY	NTPLDTBLR30~Wednesday	Low	SAFE	1	1	30	
	+	17 minutes ago	AppxAllUserStore.dll	WEDNESDAY	NTPLDTBLR30~Wednesday	Low	SAFE	1	1	BULK ACTION	
	+	34 minutes ago	wofutil.dll	WEDNESDAY	NTPLDTBLR30~Wednesday	Low	SAFE	1	1	Allow All	
	+	35 minutes ago	LanguageOverlayServer.dll	WEDNESDAY	NTPLDTBLR30~Wednesday	Low	SAFE	1	1	Deny All	
	(+)	37 minutes ann	CRYPTNET DU	WEDNESDAY	NTPI DTRI R30Wednesday	Low	SAFF	1			

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

Color	Status	Description
Red 0	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 0	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.

Terminated X Clear All X							Overview
Pending Analyst Review: 0				- Cont			463 Pending Processes
i chang relager terten e				Search		Hename • • • • • •	TERMINATED
File Found Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places	U
							NOT TERMINATED 463
Page Size 25 V	f 0 60 >						DORMANT O
Action Taken Processes: 0				Search		File Name V Q, Q,	BULK ACTION Allow All Deny All
Action Taken Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places	Acknowledge All

• **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.

Not	Termin	ated 🗙										Overview		
-		_										840 Pending Processes		
Pendi	ing A	nalyst	Review:810				Search	File N	ame 🗸	Q,	Q,	TERMINATED	0	
]		File Found Time	File Name	Location Nam	me Sensor	Asset Val	lue Opinion	Places			0		
]	+	4 minutes ago	NOTEPAD.EXE	EventTracker	R1S5-VM6	Serious	SAFE	1		1	NOT TERMINATED	0	
]	+	41 minutes ago	System.Runtime.nl.dll	EventTracker	R155-VM6	Serious	SAFE	1		1	810.		
]	+	1 hours ago	sppc.dll	EventTracker	R155-VM6	Serious	SAFE	1		1	DORMANT	0	
]	+	1 hours ago	SLC.dll	EventTracker	R1S5-VM6	Serious	SAFE	1		1	30		
]	+	1 hours ago	usinit.dll	EventTracker	R155-VM6	Serious	SAFE	1		1	BULKACTION		
]	+	1 hours ago	kbdus.dll	EventTracker	R1SS-VM6	Serious	SAFE	1		1	Allow A		
	1	+	1 hours ago	SXS.DLL	EventTracker	R155-VM6	Serious	SAFE	1		1	1000 10	·	
]	+	1 hours ago	ploptin.dll	WEDNESDAY	NTPLDTBLR30	0~Wednesday Low	SAFE	1		1	Deny Al	<u> </u>	



• **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.

orrea	et X										Overview	
din	g Ar	alyst Review:9,	892		14	ieste	Fil	Nerve	v Q	Q,	17,921 Pending Proces	1585
0		File Found Time	File Name	Location Name	Sensor	Ass	et Value	Opinion	Places		0	
	(3	10 hours ago	WhiteboardWRT ave	Text_EDR	NTPLOTBLR50-DEEPA	K Lee		SAFE	2	÷	NOT TERMINATED	6
	•	10 hours ago	WhiteboardWRT.dll	Test,EDR	NTPLOTBLRSP-DEEPA	K Les		UNKNOWN	1	T	8,122	
	Ð	10 hours age	YourPhone YPP.dll	Test_EDR	NTPLOTBLRSP-DEEPA	K Lee		SAFE	3	1	DORMANT	
	۲	10 hours ago	YourPhone.AppCore.dll	Test_EDR	NTPLOTBLRS9-DEEPA	K Les	×	SAFE	1	1.	9,892	
	Œ	10 hours ago	PhoneCommunicationAppService.dll	Test_EDR	NTPLOTBLR59~DEEPA	K Low	×	SAFE	3	1		
	(\mathbf{f})	10 hours ago	YouPhoneEerververe	Test, IDR	NTPLOTBLR59-DEEPA	IK Lee	r - 1	SME	3	÷.	4800 Million	_
	\oplus	10 hours ago	Newtonsoft.Json.Dill	Test_EDR	NTPLOTBLRSP-DEEPA	IK Les		SAFE	3	1	Albertel	
	۲	10 hours age	ScnueMinoring.dll	Test_EDR	NTPLOTBLRSP-DEEPA	K Les		SAFE	1	ŧ	Orry Al	
		10 hours age	(Ibnanoapi.dl)	Test_EDR	NTPLOTBLR39-DEEPA	K Los		SAVE	3	1		
		10 hours age	YourPhoneJexe	Test_EDR	NTPLOTBLR59-DEEPA	K Les		SAFE	3	ŧ		
	\odot	10 hours ago	microsoft.msn.weather.dll	Text_EDR	NTPLOTBLRSP-DEEPA	K Lee		SAFE	3	ł		
	(\overline{z})	10 hours ago	YourPhone.YPP.ServicesClient.dll	Text,EDR	NTPLOTBLR5P-DEEPA	K Lee		SAFE	3	Ŧ		
	\oplus	12 hours age	Polly-dl	Test_SDR	NTPLOTBLRS9-DEEPH	IK Lee		SAFE	1	1		
-	(32)		More all Max Manuall	Yest 570	AUTOR OTHER PART OFFICE							

BULK ACTION

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

BULK ACTION	
Allow All	
Deny All	

- 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.

P	endina	Analyst R	eview:863				Caurch		Ele Name V	0 0	Verview	
	chang	/ and you have					Search		riie Name V	4 4	863 Pending Processes	
			File Found Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places		TERMINATED	0
	\square	+	2 hours ago	App_Web_h54xvqhw.dll	EventTracker	R155-VM6	Serious	UNKNOWN	1	1	0	
		+	2 hours ago	pcwum.dll	EventTracker	R155-VM6	Serious	SAFE	1	1		
		+	2 hours ago	thumbcache.dll	EventTracker	R1S5-VM6	Serious	SAFE	1	:	822	
		+	2 hours ago	twinapi.dll	EventTracker	R1S5-VM6	Serious	SAFE	1	-	000	
		+	2 hours ago	CREDUI.DLL	EventTracker	R155-VM6	Serious	SAFE	1	1	DORMANT	0
		+	2 hours ago	atthunk.dll	EventTracker	R155-VM6	Serious	SAFE	1	1	30	
		+	2 hours ago	d3d10warp.dll	EventTracker	R155-VM6	Serious	SAFE	1	1	BULK ACTION	
		+	2 hours ago	pnptsdil	EventTracker	R155-VM6	Serious	SAFE	1	1	Allow Selected	
		+	2 hours ago	d2d1.dll	EventTracker	R155-VM6	Serious	SAFE	1	1	Deny Selected	



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.

Action	Take	n Processes: 3.8	88			Courch		File Name		0	Overview
		Action Taken Time	File Name	Location Name	Sensor	Scoterin	File Na A Sensor	me Name	ce	~	3888 Action Taken Processes
	\oplus	21 hours ago	MSSPH.DLL	CHETHAN	NTPLDTBLR30~Chethan		L Hash		1	:	Acknowledge All
	\oplus	21 hours ago	ShellCommonCommonProxyStub.dll	CHETHAN	NTPLDTBLR30~Chethan		L Locatio	on	1	:	
	\oplus	21 hours ago	NOTEPAD.EXE	MONDAY	R1S3VM2~MONDAY		F Produc	t Name	1	3	
	(\pm)	22 hours ago	inputswitch.dll	NTPL	NTPLDTBLR81		L Signed	Ву	1	8	
	+	22 hours ago	schtasks.exe	ANIMESH	NTPLDTBLR24.ntpl.local~ANI	MESH	L File Pat	th	1	:	
	(\pm)	Aug 22 06:32:49 AM	dinput8.dll	CHETHAN	NTPLDTBLR30~Chethan		L Parent	Process Path Process Name		:	
	\oplus	Aug 22 06:32:48 AM	CRYPTUI.DLL	CHETHAN	NTPLDTBLR30~Chethan		L Parent	Process Hash	1	:	
	÷	Aug 22 06:32:47 AM	WS2HELP.DLL	CHETHAN	NTPLDTBLR30~Chethan		Low	SAFE	1	;	
	(\pm)	Aug 22 06:32:46 AM	comres.dll	CHETHAN	NTPLDTBLR30~Chethan		Low	SAFE	1	:	
	(\pm)	Aug 22 04:23:44 AM	DEFRAG.EXE	EventTracker	ETTVMBLR22019-4		Serious	SAFE	1	:	
	\oplus	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.

Action Take	en Processes: 1				Search	98	File Name	~ Q Q
	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	:

Action Take	en Time	File Name	Location Name	Ser	nsor A	sset Value	Opinion	Places
Apr 03 04:07	7:34 PM	Wldap32.dll	Default	R1:	55-VM9 Lo	w	SAFE	1
560049 P ADDRESS OGTIME Apr 03 04:07:34 PM :CONTACT	172.28.9.15 COMPUTER R155-VM9	3 FILE NAMES FILE VERSION PRODUCT NAME SIGNED BY COUNTER SIGNED BY SIGNED ON FILE MODIFIED TIME	10.0.17134.1 Microsoft⊛ W N/A N/A Apr 03 04:07:3	findows⊗ Operatin ∺4 PM	ig System		Detected on se R155-VM9 Acknow	vledge Allow Deny Research
Launched by: DOMAIN	USERNAME	FILE PATH	C:\Windows\S svchost.exe	ystem32\WIdap32	dll			
Actions Taken History View	/ / w Now	1 MDS CHECKSUM Sda293fe9bbabdef5b VIRUSTOTAL LINK https://www.virustota b011926f/analysis/15/	03874a137ba86cd Il.com/file/4a261af 54157960/	HASH OPINION SAFE bcd280d2457dd97	OPINION REFERENCE VirusTotal '4ac5ddf18eb866b460	VIRUSTOTAL RATIO 0/65 115f391a513dc6172		A
		Threat Engine: IBM X	(FE MalcOde Team	Cymru				G

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.

		Actior Time	Taken	File Name
		Dec 20 PM	05:01:05	firefox.exe
	N/A	A, O		
	IP Ac	ddress Time	Computer	172.28.9.5
	Dec	20 05:01:05 PM	(TTAKE)	122019-3
				E
	Lau Dor NT	m ched by: main TPL	User Name prathik.g	
	Act	tions Taken Histo	ory	0
		Viev	v Now	
ime Ad	ction Taken		Grou	p(s)
Aar 13 06:20:24 PM Al	llowed		1 G	roups

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 <u>www.netsurion.com</u>.

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