# Netsurion. EventTracker®

# Endpoint Detection and Response (EDR) EventTracker v9.x

Publication Date: January 15, 2021

### Abstract

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

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

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

EventTracker's EDR capabilities mainly include:

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

### Audience

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

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



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

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

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

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

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

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

## Table of Contents

1.	Endpoint Detection and Response							
2.	Uses of EDR 4							
3.	EI	EDR vs Anti-virus						
4.	In	Introducing EDR in EventTracker v9.x						
5.	A	Accessing the EDR from EventTracker						
6.	D	ashbo	ard	8				
(	5.1	Gro	pups Pane	9				
(	5.2	Ove	erview of sensors in Groups Pane1	1				
(	5.3	Pen	iding Analyst Review pane1	3				
(	6.4	Ove	erview of the Pending Processes	0				
(	6.5	Acti	ion Taken Processes Pane	3				
(	5.6	Ove	erview of the Action Taken Processes2	5				
7.	Pi	rocess	es page2!	5				
-	7.1	Ven	ndors	6				
	7.	.1.1	Observed Vendors	8				
	7.	.1.2	Collection	2				
	7.	.1.3	Approved Vendors	3				
	7.	.1.4	Approved Collection	4				
	7.	.1.5	Import Vendors	6				
	7.	.1.6	Export Vendors	6				
-	7.2	Rule	es	7				
-	7.3	Allo	owed Process	8				
-	7.4	Den	nied Process	1				
-	7.5	Res	earch Process	3				
8.	Se	ensors	page	5				
5	8.1	Edit	t Group Info	7				
8	8.2	Edit	t Sensor Info	0				
9.	A	gent R	esource Utilization	2				

## 1. Endpoint Detection and Response

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

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

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

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

## 2. Uses of EDR

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

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

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

## 3. EDR vs Anti-virus

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

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



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

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

## 4. Introducing EDR in EventTracker v9.x

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

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

Endpoint Detection and Response services include the following:

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

## 5. Accessing the EDR from EventTracker

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





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



Figure 2

EventTracker EDR Dashboard opens (Figure 3).

baoddie									· / for the best of
10 10000	2								
Intel Services	ð								Overview
deser.									Seriers
				Barch,			Sear Q	- Q,	6.217941
INCASO .								2 Date	3
									And a historical
Transfer								1 failed	2
WONCOU								1 Total	
Default								87.4al	
OTVERME.								1.1+4	
Page Same (2)	v] + (t	d 1 00 4							
ending Ana)	pit Review 820			- Inch		100.0	and to be	a a	Overview
D	Me front lines	The Name	Incident Name		And Shee	Optimize	flam		CTCD and other strength
0 0	11 minutes apr	Pripal	WONELDH	NPUTLOD-Bedrecky	ine .	SATE	1	1	0
0 0	11 winde apr	energy and the second s	wowoole	NPATROD-Behavily	ini.	544		1	And the second s
0.0	11 minute apr	Preside	wsonaccow	NOLUTION-Behavior	i en	SATE		1	790
0 10	31 minutes ago	Action of a	WONCOM	NVX278.630-Redninkey	104	sui		1	DOBANA
0 0	34-minutes ager	wybuit	M0H8000W	1/171.010.430Michaelay	lim	544		-	40
	40 minutes Apri	LegPendedt	wowcow	N79_278.00-Biologia	1.0 m	SME			Rear address
0 0	Al months and	Annalestication for the	WONDOW	NTATE AND REPORT	100	1441		-	Aller M
	M-minutes age	Referated	WENEDW	N75.270.00-materia	100	544		-	Dec M
0 0	S2 winder age	exempted.	WONDOW	N79,278,000-Biologia	1.0mm	SAVE		1	
0 0	Sé minutes ago	Splet Nametanial	WONDOW	WIRDINGO-midwalay	100	144		1	
0 8	Sel minutes age	System Ramone Westmechantene U. Serie voll	woncow	NTR/210.430-methoday	3.64	SME		1	
0 0	54 minutes ager	Typeners/Xee/ci.28	WEINEDOW	1/174.0100.430-minutesette	100	544		1	
	Si minutes ago	Window Anoghun and	WONEDH	WPUTROD-Bidwing	1,0m	SAT			
0 -	Seminutes ego	ana but	WONCOW	NTROTOXU-mid-eutry	100	544		-	
0 0	Sectore age	Weathers Data around	WONDOW	NOVER DOC - Heatman by	100	SAR			
0.0	Sil minutes ago	ptothenall	WONCOM	WHUTEUOD-mainering	1.m	SAR		-	
0 =	Sé minutes ago	Selection and a selection of the	WEHCOW	NTADTOXIC-Wednesday	1ee	144		1	
0 *	Secondaria age	Windows Daning winned	wonester	N7N2180,830-Wednesday	100	SME		1	
0 0	Sé minutes ago	Windows Devices arrived	withdoor	NPUMLO-Indexing	lim	SAVE		1	
0 8	Skininuka ago	Window Repairing	WONCOM	NPUMUCO-melanity	100	SAR		1	
0 =	54 minutes ago	Windows (Salving)	WONCIDE	WPUPEDO-Indvasiay	liter	1441		-	
0.0	Ministrative sign	Wrothing Frieddom arrend	wentster	NSLITEAU-Industry	204	SME			
Net Ser in	v i I	(a) (a) (		La provincia de la composición de la composicinde la composición de la composición de la composición d		202	tis have = C	1 9.	Overview
12			100000		0200				O.Across. Spinyi Processon
Actes	Liden Time	The Rysler	La plue Rand	Seener Anat Salar	-		Plan		Advortinge H
Bare Line 11		w/ a   ap   a							

Figure 3





## 6. Dashboard

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

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

The three panes are the following:

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

The three Overview panels are the following:

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



al faire								
Ing Second	š.							Overview
deser.								Series
				Baich,			0mp - Q, Q,	6.07794
PROMOVE.							0 1 2 1 4 4	3
Lations							a the	AGNA REPORTING
								2
workcore							a third	
Default							@Tutal	
OTVERING.							O 1 2+44	
Page Size 21	el e le	e 1 00 1 1						
mding Analy	ot Review 820			1.00		-	~ ~ Q Q	Detroitee
			1	2014	2000			B20 Panging Pressure
0 =	II winder and	Refer al	WOMPONE AND	NRUTHARD Belleville	Log .	SAT	1	Table of the second sec
0.0	11 windle day	dial at	wowcow	NPUTROD-Behavior	ite.	SWE	4	0
0 0	El estudo apr	Parchalt	woncow	NOLITILAN-Behavity	ine .	SATE		ACT THREE COL
0 11	31 minutes ago	Advanced	WINCOM	N75278.630-Rednavlay	304	swi	(8) E	790
0 0	34 minutes ago	- mpice of	WEIHEIDDHE	NTN,070,020-mid-accia	389	SAN	+ I	DORALIVI
0 0	40 minutes age	LogProvide dil	WONCOW	NPUTROD-Behavity	100	SAVE	4) E	101
0 0	Al months ago	ang di	WONCOM	WPL010.00-mid-makey	Los	544	1 1	BLEX ACTON
0 0	All minutes ago	AppulaptionalityTrapies.40	WONCOM	N7A278LK30-Rednikeley	504	SMI		Alter Alt
0 -	N mondae age	Pur sole of	WONDOW	NTACTO CO-madranese	100	544		Day M
	Standard age	Table Distance of P	wither or	WTR.070.830. Weinesing	100	141		
0	Secondaria age	Sectors Response Westmanhasters (Classica)	woncow	NTATERAN-Instructor	104	SME	6 1	
0 0	Sé minutes ager	Nation Xoria all	WEINESSHE	N75,070,020-midweite	100	544	8 B	
0 0	St minutes ago	Ministers Perceptus animal	WONDOW	NPATEROD-Belowing	1.1-	SAR	- E	
0 0	Sé minutes espr	setup in all	WONCOW	N7A276X01-mid-makey	100	544	F 1	
0	Service age	Westing Data around	WONDOW	N74218LAN-Inducing	2.04	SME		
0 0	54 minutes ager	Whiteen Distalization where	WEINEDOW	NTA2TE-OO-multimates	100	544		
0 0	Si minutes ago	propriate (8	WONCOM	NPUTLOD-Behavity	Um.	544		
0 -	Se monutes app	Winter Series and	windlas	ACR. COLUMN & M. Machaelan	100	1441		
0 0	Si minuter and	Windows Device activity	WENCOW	Wh211LOb-Belleville	line	SAVE		
0 8	SA minutes ago	Windows Rith winning	WONDOW	WHUTEUGD-Biologies	100	SAR	4	
0 0	St minutes ago	Winters (Carried	wowcow	WPUPILOD-Indvallay	Line	SAVE	a. 1	
0 8	Strends age	Window Franklahm arrend	wonester	NPL218,430-metworks	344	SME	(A) B	
0 0	Strindings	000000000 ( + )	withdow	NOLITI, KIA-Badmaing	1.0m	SAT.		
Action Taken	Processes 0			- Look		5	in have = Q, Q,	Overview
Action	Taken Time	Pile Name Location 1	-	Seemer Asset Value		ie :	Parm	Concerning and the second
has been at								Advantage N
		A(* (@)(*)						



### 6.1 Groups Pane

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

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

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

Groups			
	Search	Group	Q Q
Default		Sensor	🕽 🕢 4 Total
EventTracker			🕽 🚹 1 Total
NTPL		•	1 Total
PRISM		C	1 Total

Figure 5

• Each color indicates a Group status.

			Sensors
Search Grou	p v Q Q	2	ALERTING
		^	11
	1 2 Total		
Status 🕳	1 Total		NON REPORTING
	1 1 Total		3
	Search Grou Status —	Search Group V Q Q 1 2 Total Status 1 1 Total 1 1 Total 1 1 Total	Search Group V Q Q Q Status 1 1 Total 1 1 Total

Figure 6

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

Color	Status	Description
Yellow <sup>1</sup>	ALERTING	This status shows all the locations or systems where a new process has appeared.
Gray 1	NON-REPORTING	This status shows that we have not received a 'keep alive' status from there systems or locations.

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



PRISMSYSGroup			1 2 Total
CONTACT NAME CONTACT PHONE	CONTACT EMAIL		
R 54-V M3~Pri ∋sys - Win 8.1		Process status of the	000
N PLD I LR30- ris sys - Win 10	Sensors	sensors	

#### Figure 7

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

Color	Status	Description		
Orange 🧿	DORMANT	Indicates the number of files detected before execution.		
Red 🧿	TERMINATED	Indicates the Terminated process by the EventTracker EDR.		
Fountain Blue 0	NOT TERMINATED	Indicates the process that ran during the maintenance mode and is now running without disposition.		

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

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

PRISMSYS	1 2 Total
CONTACT NAME CONTACT PHONE CONTACT EMAIL	
K154-VW5~PTISTISYS - VVIII 0.1	000
NITHINTELD20 Discorp WE 10	

Figure 8

### 6.2 Overview of sensors in Groups Pane

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



≡	Niksurion, Eventilischer						
•	Dashboard				<b>†</b> /5	rentTrackerEDR./I	Jush
•: 	Total Sensors: 15			0	verview		
	Groups	- Avera			Sensors		
	F 855MSY	Starch_	0100p V 64		CDO ING	11	
	E-entities or		👔 1 Tati	- 1	ION REPORTING	3	-
	P EDIAES AV		1 Tot	Ľ		<u> </u>	



Color	Status	Description
Yellow <sup>1</sup>	ALERTING	This status shows all the locations or systems where a new process has appeared.
Gray 1	NON-REPORTING	This status shows that we have not received a 'keep alive' status from there systems or locations.

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

=	Nikwise, Sortholar		•
•	Dashboard		🖈 / EventTrackerEDR / Dashbox
•	Total Sensors: 15		Overview
	Aberling 🗶 Cour AB 🗶		Sensors
	Groups		11
		Seach. deep V Q, Q,	
	R M*S	🛈 🕦 2 Setal	NON REPORTING 0
	et militer	(j) 1 Tetal	
	O.N.A.	(j) 1 Tetal	
	0.141	(1) 1 Tetal	
	A/ A	(1) 1 Total	
	0 AV A.3	(1) 1 Seal	
	N VE H	1 Total	



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



venthackerEDR / Dashb
11
3

Figure 11

## 6.3 Pending Analyst Review pane

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

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

Pendin	g Anal	yst Review:10,687	,		Search		File Name Sensor Name	Q	Q
		File Found Time	File Name	Location Name	Sensor	Asset Value	Hash Location		
	$\left(+\right)$	a minute ago	dosvc.dll	AI SH	N" PLE "B" R24~# IIMES H	Low	Opinion Product Name		÷
	$\left(+\right)$	a minute ago	III on b	AI SH	N" PLE "B 324~# IIMES 1	Low	Signed By File Path		÷
	$\left(+\right)$	2 minutes ago	n d. sys	AI SH	N" PLE "B 324~/ IIMES 1	Low	Parent Process Path		:
	$\left(+\right)$	2 minutes ago	w pc .dll	AI SH	N" PLE "B R24~# IIMES H	Low	UNKNOWN 1		÷
	$\left  + \right $	4 minutes ago	ui bk 1.dll	AI SH	N" PLE "B 324~/ IIMES 1	Low	UNKNOWN 2		:
	+	6 minutes ago	A p_' :b_oa25k2ei.dll	M H J	ET VN 3L 22012 3~my hili	High	UNKNOWN 1		÷

#### Figure 12

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



		File Found Time	File Name	Location Name	Sensor			Asset Value	Opinion	Allow
	+	0 minutes ago	dosvc.dll	' EDN <sup>-</sup> SDAY	N PLDT		day	Low		Deny
	$\left +\right $	6 minutes ago	NTL INMA .DLL	AIME 3H	N PLDT	.R24~# NIMI	н	Low	UNKNOWN	Research
	+	6 minutes ago	drp: >v.dll	, JIME 3H	N PLDT	.R24~# NIMI	н	Low	UNKNOWN	1
	$\left +\right $	7 minutes ago	mrx lav.sys	11ME 3H	N PLDT	.R24~# NIMI	н	Low	UNKNOWN	1
	+	7 minutes ago	web :Int.dl	, JIME 3H	N PLDT	R24~F NIMI	н	Low	UNKNOWN	1
	$\left  + \right $	9 minutes ago	uirił bon.d	11ME 3H	N PLDT	.R24~# NIMI	н	Low	UNKNOWN	2
	$\left. + \right.$	11 minutes ago	App. Web_ 125k2ei.dll	I ITTI I	e (VME	₹22012 3~n	thili	High	UNKNOWN	1
	+	11 minutes ago	Apr Web_ /kmiqh.dll	Т АТНІ І	e (VME	₹22012 3~n	thili	High	UNKNOWN	1
	$\left +\right $	11 minutes ago	msj toledt 0.dll	Т ТНІ І	e (VME	₹22012 3~n	thili	High	UNKNOWN	3
	$\left +\right $	11 minutes ago	QUI RY.DLI	, vime iH	N PLDT	.R24~/ NIMI	н	Low	SAFE	2
7	(+)	12 minutes ago	Apr. Web apuo2et.dll	LYTHI J	E IVME	₹22012 3~n	thili	High	UNKNOWN	1

Figure 13

#### Allowing the process

1. Click Allow, Allow Process dialog box opens.

Allow Process				×
File Name: Signed by:	dosvc.dll N/A	Opinion:	UNKNOWN	
	Global 🕲		Select Group	
add comments here	2			
				Allow



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

Allow Process	2			×
File Name: Signed by:	dosvc.dll N/A	Opinion:	UNKNOWN	
	Global 🕲		Select Group 9	
add comments	here			

Figure 15



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

File Name:	dosvc.dll			
Signed by:	N/A	Opinion:	UNKNOWN	
	Ciebel 🔿		Select Genue 0	
ailable Groups		Selected	Groups	
Win 7 and Server 2 Win XP and Server Domain Controller Firewall Devices Network Devices VmWare A28 After Dark Airlines Allensolly AmericanExpress Armani Arsenal BangaloreCentral Barcelona	008 Above 2003 rs	×		
ld comments here.				A

#### Figure 16

#### **Denying the process**

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

Deny Process				
File Name:	dosvc.dll			
Signed by:	N/A	Opinion:	UNKNOWN	
	Global 🕲		Select Group 오	
dd comments here				
				Deny



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



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

File Name:	dosvc.dll	0.11		
Signed by:	N/A	Opinion:		
	CI L 140			
1.1.1.0	Global 🕲	State 10	Select Group V	
Allensolly AmericanExpress Armani Arsenal BangaloreCentral Barcelona BeingHuman BigBazar Blackberry Blenders Pride BrandFactory Burberry Carvir-ESP Carvir-USA		∧ → <p< td=""><td></td><td></td></p<>		
ld comments here				



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

The Process tab is discussed in detail in the Processes Section.

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

• Click 🗄 to know more about the process details.

Ac	tion Tak	en Processes: 29				Search		File Name $\sim$	Q,	Q	Overview
		Action Taken Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places			29 Action Taken Processes
	+	Mar 20 04:14:10 PM	sppsvc.exe	WEDNESDAY	NTPLDTBLR30~Wednesday	Low	SAFE	1		÷	Acknowledge All
	+	Mar 20 04:14:09 PM	App_Web_un5gxqrj.dll	Test_EDR	NTPLDTBLR59~DEEPAK	Low	UNKNOWN	1		÷	
	+	Mar 20 04:14:09 PM	App_Web_vzxilcdh.dll	Test_EDR	NTPLDTBLR59~DEEPAK	Low	UNKNOWN	1		÷	

Figure 19

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



🗌 🖯 6 hours ago dstokenclear	n,exe	NTPL ETTVMBLR2W10-2 Low		SAFE 2	I	2 1,40 I Pending Processes
Thank 400505	1 File Names			Detected on sensors 2	2	TERMINATED 115
1P 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	1	ETTVMBLR22019-44ug 17 06:23:44 PM		9,089
Contact	Counter Signed By	N/A				DORMANT
	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	1			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	1			
	Hash	6a7d8561bcba33ed64e3befd67c10ca0				

Figure 20

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

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

🗌 🗇 6 hours ago dstokenclear	n.exe	NTPL ETTVMBLR2W10-2	Low	SAFE	2		Ξ	21,401 Pending Processes
Thank 400606	1 File Names			Detected on sensors			2	TERMINATED
IP Address 172.28.9,164	File Version	10.0.17763.1		ETTVMBLR2W10-2	6 ho	urs ago		NOT TERMINATED
Log Time Computer Sep 01 07:57:18 AM ETTVMBLR2W10-2	Product Name Signed By	Microsoft® Windows® Operating System	ų	ETTVMBLR22019-44	kug 17 06:21 PM	3.44		9,089
Contact	Counter Signed By	N/A						DORMANT
	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	eny					Allow All
Observation Process does not match the allowed process criteria.	Parent Process Path	C:\Windows\System32\svchost.exe	eny					Deny All
	Parent Process Hash	23e47ce30cfc49f60a6e24b50aa83b9b						
	File Path	C:\Windows\system32\dstokenclean.exe	eny 🔲					
	Hash	6a7d8561bcba33ed64e3befd67c10ca0						

Figure 21

#### NOTE:

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

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

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

nding Analyst Review:12,589			Search	File Name	~ Q	Q	Overview
D 1 hours App_Web_jzh5vxid.     ago	dii Ev	entTracker 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         ETTVMBLR22019-4           Contact         Contact	1 File Names File Version Droduct Name Signed By Counter Stored By N/A			Detected on sensors ETTVMBLR22019-4	1 hours ago	1	93 NOT TERMINATED 0 251 DORMANT 0
Launched by: Domain User Name NT AUTHORITY NETWORK SERVICE	Signed On File Modified Time Sep 04 Parent Process Name W3wp.e	10:30:54 AM					12,250 BULK ACTION Allow All
Observation Process loaded a binary that does not match the allowed criteria.	Parent Process Path C:\Wind	dows\SysWOW64\inetsrv\w3wp.exe	ow Deny				Deny All
	Parent Process Hash 3c4949; File Path C:\Win y ASP.N zh5vxid	2762be5985185665a7202c4dda dows\Microsoft.NET\Framework\v4.0 Ef Files\eventtracker\29c5a12a\b40dr I.dll	30319\Temporar 16bb\App_Web_j ow Deny ]				
	Hash f92b34b	8bc281a87b43c93d1b0bcdc1e					

Figure 22

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



Pending Analyst Review:12,589			Search File Name V Q Q Overview
1 hours App_Web_jzh5vxid. ago	111	EventTracker ETTVMBLR22019-4	Serious UNKNOWN 1 : 12,589 Pending Processes TERMINATED
Thane, 400606 IP Address 172.28.9.147 Log Time Computer Sep 04 10:30:54 AM ETTVMBLR22019-4 Contact	1 File Names File Version Product Name Signed By Counter Signed By Signed On	0.0.0.0 N/A	Detected on sensors 1 ETTVMBLR22019-4 1 hours ago 251 DORMANT 0 12,250
Launched by:	File Modified Time	Sep 04 10:30:54 AM	BULK ACTION
Domain User Name NT AUTHORITY NETWORK SERVICE	Parent Process Name	w3wp.exe	
Observation	Parent Process Path	C:\Windows\SysWOW64\inetsrv\w3wp.exe	Deny All
Process loaded a binary that does not match the allowed criteria.		Allow	
	Parent Process Hash	3c49492762be5985185665a7202c4dda	
	File Path	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Ten y ASP.NET Files\eventtracker\29c5a12a\b40dd6bb\App, zh5vxid.dll Allow Deny	emporar .p_Web_j
	Hash	f92b34b8bc281a87b43c93d1b0bcdc1e	

Figure 23

#### Add rule window

• Add Rule	×
Rule Name	
w3wp.exe	
Note: Please provide the process name or folder path for rule.	
Parent Process Hash	
3c49492762be5985185665a7202c4dda	
Rule Description	
Provide rule description	
Allow child process	
Global 🕲	Select Group 🛛
	Add Close

Figure 24

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



### 6.4 Overview of the Pending Processes

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

Pendina	Analys	t Roviow 840								0	0	Overview		
rending	Analys	therew.040				Search		File Name	~	04	4	840 Pending Proc	Jesses	
		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			
	+	12 minutes ago	SLC.dll	EventTracker	R1S5-VM6		Serious	SAFE	1		÷	NOT TERMINATED		
	+	13 minutes ago	uxinit.dll	EventTracker	R1S5-VM6		Serious	SAFE	1		1	NOT TERMINATED	910	Ĭ
	+	13 minutes ago	kbdus.dll	EventTracker	R1S5-VM6		Serious	SAFE	1		÷		010	
	+	13 minutes ago	SXS.DLL	EventTracker	R1S5-VM6		Serious	SAFE	1		1	DORMANT	20	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		÷	BULK ACTION		
	+	34 minutes ago	wofutil.dll	WEDNESDAY	NTPLDTBLR30	~Wednesday	Low	SAFE	1		÷		Allow All	
	+	35 minutes ago	LanguageOverlayServer.dll	WEDNESDAY	NTPLDTBLR30	~Wednesday	Low	SAFE	1		÷		Deny All	
	(+)	37 minutes ann	CRVPTNET DI I	WEDNESDAY	NTPI DTRI R30	Werinesriav	Low	SAFE	1					



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

Color	Status	Description
Red 🤨	TERMINATED	Indicates the Terminated process by the EventTracker EDR.
Fountain Blue 0	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:** When you click on the **TERMINATE** tab, you will see all the terminated process listed in the Analyst Review pane. It filters the EDR database and displays all the events of that status.



Terminated X Clear All X							Overview
Pending Analyst Review: 0							463 Pending Processes
Tending Analyse Neview. 0				Search		File Name V Q Q	TERMINATED
File Found Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places	0
							NOT TERMINATED 0
Page Size 25 V < 1	of 0 GO >						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

#### Figure 26

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

Not Te	rmina	ated 🗙											Overview		
Pendir	g A	nalyst	Review:810				Search		File Name	~	Q	٩	840 Pending Proces	ises	0
			File Found Time	File Name	Location Name	Sensor		Asset Value	Opinion	Places				0	
		+	4 minutes ago	NOTEPAD.EXE	EventTracker	R1S5-VM6		Serious	SAFE	1		÷	NOT TERMINATED		0
		+	41 minutes ago	System.Runtime.ni.dll	EventTracker	R1S5-VM6		Serious	SAFE	1		+			
		+	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		4			
		÷	1 hours ago	uxinit.dll	EventTracker	R155-VM6		Serious	SAFE	1		1	BULK ACTION		_
		+	1 hours ago	kbdus.dll	EventTracker	R155-VM6		Serious	SAFE	1		1		Allow All	
		+	1 hours ago	SXS.DLL	EventTracker	R1S5-VM6		Serious	SAFE	1		+			$\dashv$
		+	1 hours ago	ploptin.dll	WEDNESDAY	NTPLDTBLR30	-Wednesday	Low	SAFE	1		÷		Deny All	



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



=	Nelsonion. D	entite	er)										
	Pendin	g Ar	ulyst Review 9.	892		r	Tauro h		is Flame	H Q	Q	Overview 17,323 Rending Proces	10
	0		He found line	Alle Name	Location Name	Semar		Asset Value	Opinioo	Places		0	Ĵ.
		(E)	10 hours ago	Whiteboard/WRT.ave	Text, EDH	NTPLOTBLRS4-DEE	PAK I	Lee	SAFE	1	Ŧ	NOT TERMINATED	0
		12	11 henris ago	WhitehourdWRT.dll	Test, 518	NTPLOTBLRSI-DES	Bak I	Lein	UNENOWN	2	1	8,122	
			10 News ego	YouPhone YPP JR	Text,EDR	NTPLOTIBLESH-DER	лк і	Level	SAFE	1	1	DORMANT .	0
			13 bourt age	YouPhane.AppConcill	Test,E28	NTPLOTBLRSF-DER	FRK I	Liter	SATE	1	1	9,892	
			10 Hours age	PhoneCommunicationAppGenvice.dll	Test_EEM	NTPLOTIBLESH-DEE	Pak I	Lów	SAFE	3	1		
	D	(0)	10 hours aga	YouPhonelessesate	Tet,iDH	NTPLOTBLRSH-DO	PIK I	.00	SME	1	÷	Dub, Hurson	_
		121	12 hours ago	Newtonia R. June 201	Tert,50R	NTPLOTBLRS8-DER	TRAK I	Lyie .	SAFE.	1	1	Abread	
		(3)	15 heart age	Sematheoring.dt	Test,519	NTPLOTRLRSP-DED	Dik I	Lew .	SAFE	1	1	Dun Al	
			10 hours ago	Minanuqi 201	Taxt,00R	NTPLOTELRSS-DED	PAK 1	Line .	SAFE	1	1		
			10 hours ago	YouPhone ete	Test_SDR.	NTPLOTBLRSE-DED	BK I		SAIL	1	Ŧ		
			10 hours ago	microsoft.man.veather.dll	Test,EDR	NTPLOTBLASI-DES	BK I	Loie	SAFE	1	ī		
		10	10 hours ago	YourPhone YPP ServicesClient.dll	Text,8DR	NTPLOTBLRSP-DEE	Pak I	les	SAFE	3	1		
		0	Ti keurs age	Folyall	Text_SDR	NTPLOTBLRSB-DED	IFIK I	Law	SAFE	1	1		
	0	122		In such the local diversity	Test Mark		-						



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

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





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

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



ending	Analyst Re	eview:863				Caarrh		Ella Nama 🗸 🖸	0	Overview	
						Jearcha		The Nonite	~~~	863 Pending Processes	
		File Found Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places		TERMINATED	0
	+	2 hours ago	App_Web_h54xvqhw.dll	EventTracker	R1S5-VM6	Serious	UNKNOWN	1	1	0	
	+	2 hours ago	pcwum.dll	EventTracker	R1S5-VM6	Serious	SAFE	1	1	NOT TERMINATED	
	+	2 hours ago	thumbcache.dll	EventTracker	R1S5-VM6	Serious	SAFE	1	1	833	
	+	2 hours ago	twinapi.dll	EventTracker	R1S5-VM6	Serious	SAFE	1	1	055	
	+	2 hours ago	CREDUI.DLL	EventTracker	R1S5-VM6	Serious	SAFE	1	1	DORMANT	0
	(+)	2 hours ago	atithunk.dll	EventTracker	R155-VM6	Serious	SAFE	1	1	30	
	+	2 hours ago	d3d10warp.dll	EventTracker	R1S5-VM6	Serious	SAFE	1	1	BULK ACTION	
	$(\pm)$	2 hours ago	pnpts.dll	EventTracker	R155-VM6	Serious	SAFE	1	1	Allow Selected	
	+	2 hours ago	d2d1.dll	EventTracker	R155-VM6	Serious	SAFE	1	1	Deny Selected	
_											



## 6.5 Action Taken Processes Pane

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

Action	Take	en Processes: 3,8	88			Search		File Name		0	Overview
		Action Taken Time	File Name	Location Name	Sensor	Sedicit	File N A Senso	ame r Name	ce	~	3888 Action Taken Processes
	$(\pm)$	21 hours ago	MSSPH.DLL	CHETHAN	NTPLDTBLR30~Chethan		L Hash			:	Acknowledge All
	$\oplus$	21 hours ago	ShellCommonCommonProxyStub.dll	CHETHAN	NTPLDTBLR30~Chethan		L Locati	ion	1	1	
	$\oplus$	21 hours ago	NOTEPAD.EXE	MONDAY	R1S3VM2~MONDAY		H Produ	ict Name	1	8	
	$\oplus$	22 hours ago	inputswitch.dll	NTPL	NTPLDTBLR81		L Signe	d By	1	÷	
	(+)	22 hours ago	schtasks.exe	ANIMESH	NTPLDTBLR24.ntpl.local~Al	NIMESH	L File Pa	ath	1	:	
	$(\pm)$	Aug 22 06:32:49 AM	dinput8.dll	CHETHAN	NTPLDTBLR30~Chethan		L Paren	t Process Path t Process Name	1	:	
	$(\pm)$	Aug 22 06:32:48 AM	CRYPTUI.DLL	CHETHAN	NTPLDTBLR30~Chethan		L Paren	t Process Hash	1	1	
	$(\pm)$	Aug 22 06:32:47 AM	WS2HELP.DLL	CHETHAN	NTPLDTBLR30~Chethan	6	Low	SAFE	-	;	
	$(\pm)$	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 on the 👘 icon to expand the tab. You will see the detailed information about the File Names and the corrective action taken.

Action Tal	ken Processes: 1				Searc	h	File Name 🗸	Q	Q
-	Action Taken Time	File Name	Location Name	Sensor	Asset Value	Opinion	Places		
÷	Apr 03 04:07:34 PM	Widap32.dll	Default	R1S5-VM9	Low	SAFE	1		÷
			Fi	gure 32					



Action Taken Time	File Name	Location Name	Ser	nsor A	sset Value	Opinion	Places	
Apr 03 04:07:34 PM	Wldap32.dll	Default	R15	55-VM9 Li	w	SAFE	1	
	1 FILE NAMES					Detected on	sensors	1
	FILE VERSION	10.0.17134.1				R1S5-VM9		18 Min ago
560049	PRODUCT NAME	Microsoft® Wir	ndows® Operatin	g System				
P ADDRESS 172.28.9.153	SIGNED BY	N/A				Ackn	owledge Allow D	env Research
.OGTIME COMPUTER	COUNTER SIGNED BY	N/A						
Apr 03 04:07:34 PM R1S5-VM9	SIGNED ON							
CONTACT	FILE MODIFIED TIME	Apr 03 04:07:34	PM					
La	FILE PATH	C:\Windows\Sy:	stem 32\WIdap 32.	dll				
aunched by:	PARENT PROCESS NAME	svchost.exe						
DOMAIN USERNAME NT AUTHORITY SYSTEM	PARENT PROCESS PATH	C:\Windows\Sy	stem32\svchost.e:	ke				
Actions Taken History 1								
View Now	MD5 CHECKSUM 5da293fe9bbabdef5b3	874a137ba86cd	HASH OPINION	OPINION REFERENCE VirusTotal	VIRUSTOTAL RATIO 0/65			
	VIRUSTOTAL LINK							
	https://www.virustotal b0f1926f/analysis/155	.com/file/4a261afb 4157960/	cd280d2457dd97	4ac5ddf18eb866b460	)15f391a513dc6172			Ac
	Threat Engine: IBM X	F MalcOde Team (	Vmru					Go



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

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

	Action Taker	n Time	File Name
Θ	Apr 11 05:39:	28 PM	System.Run
bangal Bengal	ore bangalore uru, 560049		
IP ADDR	223	1	69.254.181.202
LOGTIM Apr 11	E 05:39:28 PM	COMPUTER NTPLDTBLR31	~SECURITY
CONTAC mahes	er h		n=
Launch	ed by:		
DOMA NT AU	IN JTHORITY	USER NAME NETWORK SER	VICE
Action	s Taken History		1
		View Now	
		View Now	

Figure 34

Time	Action Taken	Group(s)	User	Comments	
Mar 13 06:20:24 PM	Allowed	1 Groups	s ktirr p		
Figure 35					

### 6.6 Overview of the Action Taken Processes

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

Overview
2 Action Taken Processes
Acknowledge All

Figure 36

## 7. Processes page

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

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

Proc	cesses		♠ / EventTrackerEDR
+	Vendors: 66,270	G Collections 4	Overview
+	Rules:	✓ Allowed Rules 0 × Denied Rules 0	Processes
+	Allowed Process: 2,097,495		
+	Denied Process: 2		2,097,495
+	Research Process:		2
			research O

Figure 37



The processes page will have the following:

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

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

	Processes		♠ / EventTrackerEDR / Processes
©!	+ Vendors: 66,270	Collections 4      Approved Vendors 34	Overview
	🕀 Rules:	✓ Allowed Rules 0 × Denied Rules 0	Processes
	<ul> <li>Allowed Process: 2,097,495</li> </ul>		
	Denied Process: 2		2,097,495 DENIED
	+ Research Process:		2
			research O



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

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

### 7.1 Vendors

• Click 🗉 icon on the vendor's tab.

≡	Netsurion. EventTracker			•
	Processes			↑ / EventTrackerEDR / Processe
<b>⊚</b> ! ⊒	Uendors: 2,270	ction 2 ③ Approved Vendors 30		Overview
	OBSERVED VENDORS COLLI Search Vendor Name Q Q	CTION APPROVED VENDORS APPROVED COLLEC	CTION IMPORT EXPORT Product + Create New Signer Collection	ALLOWED
	Oracle America, Inc. 18,512 SIGNER	SAP AG 16,220 SIGNER	Dassault Systemes SolidWorks Corp. 15,973 SIGNER	2,097,459 DENIED
	Apple Inc. 14,974 SIGNER	Autodesk Development Sarl     I4,947 SIGNER	Symantec Corporation	RESEARCH
	DASSAULT SYSTEMES SA     11,131 SIGNER	Cisco WebEx LLC 10.648 SIGNER	CyberLink Corp. 10.400 SIGNER	

Figure 39

The Vendors page opens with the following tabs

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

	Netsurion, EventTracker			0 -
**	Processes			♠ / EventTrackerEDR / Processes
<b>⊚</b> ! <b>□</b>	□ Vendors: 2,270			Overview
	OBSERVED VENDORS COL	LECTION APPROVED VENDORS APPROVED COLLEG	CTION IMPORT EXPORT	Processes
	Search Vendor Name Q Q	🗹 Show Signer 🗹 Show	Product + Create New Signer Collection	
	Oracle America, Inc.	SAP AG	Dassault Systemes SolidWorks Corp.	2,097,439 DENIED
	18,512 SIGNER	16,220 SIGNER	15,973 SIGNER	1
	Apple Inc.	Autodesk Development Sarl	Symantec Corporation	RESEARCH
				1
	DASSAULI SYSTEMES SA 11,131 SIGNER	Cisco Web±x LLC 10,648 SIGNER	CyberLink Corp.	

Figure 40

#### 7.1.1 Observed Vendors

• It displays all the vendors present in the environment.

≡	Netsurion EventTracker			• •
	Processes			♠ / EventTrackerEDR / Processes
©! □	□ Vendors: 2,270 🛛 😼 Colle	ection 2 ③ Approved Vendors 30		Overview
		ECTION APPROVED VENDORS APPROVED COLLE	CTION IMPORT EXPORT	Processes
	Search Vendor Name 🔍 🍳	🗷 Show Signer 🗷 Show	Product     + Create New Signer Collection	ALLOWED
	Oracle America, Inc.	SAP AG	Dassault Systemes SolidWorks Corp.	2,097,459
	18,512 SIGNER	16,220 SIGNER	15,973 SIGNER	
	Apple Inc.	Autodesk Development Sarl	Symantec Corporation	
	14,974 SIGNER	14,947 SIGNER	11,654 SIGNER	RESEARCH
	DASSAULT SYSTEMES SA	Cisco WebEx LLC	CyberLink Corp.	
	11,131 SIGNER	10,648 SIGNER	10,400 SIGNER	
		Figure 41		

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

Processes				↑ EventTrackerEDR / Processe
Vendors: 2,239	G Collection 2	Approved Vendors 30		Overview
OBSERVED		APPROVED VENDORS APPROVED	COLLECTION IMPORT EXPORT	Processes
Search Vendor Name	٩	Show Signer	Show Product + Create New Signer Co	ALLOWED
Oracle America, Inc.	0	SAP AG	Dassault Systemes SolidWorks Cor	<sub>p.</sub> 2,097,459
18,512 SIGNER	16,220	SIGNER	15,973 SIGNER	DENIED
Apple Inc.	O	Autodesk Development Sarl	Symantec Corporation	
14,974 SIGNER	14,947	SIGNER	11,655 SIGNER	RESEARCH
DASSAULT SYSTEMES SA		Cisco WebEx LLC	CyberLink Corp.	1
11,131 SIGNER	10,648	SIGNER	10,400 SIGNER	

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

Netsurion. EventTracker	• •
Processes	↑ EventTrackerEDR / Processes
Vendors: 31     Image: Collection 2     Image: Approved Vendors 30	Overview
OBSERVED VENDORS COLLECTION APPROVED VENDORS APPROVED COLLECTION IMPORT EXPORT	Processes
Search Vendor Name 🔍 🔍 🔲 Show Signer 🐨 Show Product + Create New Signer Collection	2 097 459
Google Chrome     FortiClient support library     FortiClient FDS protocol engine       PRODUCT     PRODUCT     PRODUCT	DENIED
FortiClient Customized Resource     Microsoft® Speech Recognizer 11.1     Internet Explorer	1
PRODUCT PRODUCT PRODUCT	RESEARCH
HashMyFiles     Microsoft Edge Web Platform     Windows Installer - Unicode	1
PRODUCT PRODUCT PRODUCT	

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

letsurion. EventTracker			0 •
Processes			♠ / EventTrackerEDR / Processes
□ Vendors: 2,270	lection 2 🙂 Approved Vendors 30		Overview
OBSERVED VENDORS CO	LECTION APPROVED VENDORS APPROVED COLI	ECTION IMPORT EXPORT	Processes
Search Vendor Name	🕑 Show Signer 🕑 Sho	w Product + Create New Signer Collection	
Oracle America, Inc.	SAP AG	Dassault Systemes SolidWorks Corp.	2,097,459
18,512 SIGNER	16,220 SIGNER	15,973 SIGNER	
Apple Inc.	Autodesk Development Sarl	Symantec Corporation	
14,974 SIGNER	14,947 SIGNER	11,655 SIGNER	RESEARCH
DASSAULT SYSTEMES SA	G Cisco WebEx LLC	CyberLink Corp.	1
11,131 SIGNER	10,648 SIGNER	10,400 SIGNER	
	etsurion. Eventifracker Processes Vendors: 2,270 2 Col OBSERVED VENDORS COL Search Vendor Name Q Q Oracle America, Inc. 18,512 SIGNER Oracle America, Inc. 18,512 SIGNER O Apple Inc. 14,974 SIGNER O DASSAULT SYSTEMES SA 11,131 SIGNER	etsurion. EventTracker         Processes         Image: Search Vendors: 2,270         Image: Search Vendor: 2,270	etsurion. EventTracker         Processes         Image: Search Vendors: 2,270       Image: Search Vendors 30         Image: Search Vendor Name       Image: Search Vendor Name         Image: Search Vendor Name       Image: Search Vendor Name

Figure 44



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

≡	Netsurion. Eventīracker			• •
**	Processes			♠ / EventTrackerEDR / Processes
<b>⊗</b> !	Vendors: 2,270 G College	ction 2 (a) Approved Vendors 30		Overview
	OBSERVED VENDORS COLLE	CTION APPROVED VENDORS APPROVED COLLEC	TION IMPORT EXPORT	Processes
	Search Vendor Name Q Q	🕑 Show Signer 🕑 Show	Product + Create New Signer Collection	2,097,459
	Oracle America, Inc.  18,512 SIGNER	SAP AG 16.220 SIGNER	Dassault Systemes SolidWorks Corp.	DENIED
	C Apple Inc.	Autodesk Development Sarl	Symantec Corporation	1
	14,974 SIGNER	14,947 SIGNER	11,655 SIGNER	RESEARCH 1
	DASSAULT SYSTEMES SA	Cisco WebEx LLC 10.648 SIGNER	CyberLink Corp.	
		Figure 45		

To create or edit vendor group:

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

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

Test		×
vailable Vendor	Selected Vendor	
Refine Search	Refine Search	
Antir3.Runtime		
Beyond Compare	•	
Clip		
EventTracker	••	
FortiClient Auto-update A		
FortiClient Customized Re		
FortiClient FDS protocol		
FortiClient support libra	~	
		Save
	Figure 46	



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

ndor Collection Name		
Test		
wailable Vendor	Selected Vendor	
Refine Search	Refine Search	
Beyond Compare	Antir3.Runtime	^
EventTracker	Clip	
FortiClient Auto-update A	FortiClient FDS protocol	
FortiClient Customized Re		
FortiClient support libra		
Gracenote SDK		
Grammarly for Microsoft®		
Internet Explorer	~	~



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

Add Vendor Collection		×
Vendor Collection Name		
Available Vendor EventTracker	Selected Vendor Refine Search	
EventTracker	Antir3.Runtime	^
	Clip FartiClient FDS protocol	
	~	
	×	~
		Save
	Figure 48	



1. To unselect the vendors from collection, click 📩 icon in the Selected Vendor list.

- 2. To unselect multiple vendors, click icon.
- 3. Click Save.

ailable Vendor	Selected V	/endor
Refine Search	Refine S	iearch
Antir3.Runtime	Antir3.R	luntime
Beyond Compare	• Clip	
Clip	FortiClie	ent FDS protocol
EventTracker		
FortiClient Auto-update Agent		
FortiClient Customized Resource		
FortiClient FDS protocol engine		
FortiClient support library	v	

#### 7.1.2 Collection

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

Processes		♠ / EventTrackerEDR / Processes
Processes	tion 2 ② Approved Vendors 30  TION APPROVED VENDORS APPROVED COLLECTION IMPORT EXPORT  + Create New Signer Collection  Testing Collection2  Process Count  2.024 Vendor Count  3	Overview Processes ALLOWED 2,097,459 DENIED 1 RESEARCH 1
Page Size 25 V < 1 of 1		

Figure 50

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

endor Collection Name		
Testing Collection1+		
Available Vendor	Selected Vendor	
Intel(R) Software Development Products	3Dconnexion Inc	^
JPMorgan Chase Bank, N.A.	3Dconnexion Inc.	
.NET Foundation	3Dconnexion SAM	
{E47B900D-10F3-4A03-981A-73B8360F243A}		
16 Software		
20-20 Technologies Inc.		
2BrightSparks Pte Ltd		
360.cn	~	~
360.cn	V	~



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

#### 7.1.3 Approved Vendors

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

Vendors: 2,265		g Collection 2 (2) Approved Vendors 30				
		OBSERVED VENDORS COLLECTION APPROVED VEN	OORS APPROVED COLLECTION IMPORT EXPOR	т		
Search Approved Vendor Name	Q,					
25308 Adobe Systems Incorporated	1	10996 Microsoft Windows Hardware Compatibility Publ 🧭	9839 Hewlett-Packard Company	1	3468 Intel Corporation-Mobile Wireless Group	
SIGNER		SIGNER	SIGNER		SIGNER	
1318 Microsoft Windows Kits Publisher	Ø	871 Microsoft Windows	363 Microsoft Corporation	Ø	251 Microsoft Windows Publisher	
SIGNER		SIGNER	SIGNER		SIGNER	
237 Microsoft Windows Third Party Application Com	Ø	185 Microsoft Windows Component Publisher 🧭	78 Microsoft 3rd Party Application Component	1	66 Microsoft Windows 3rd party Component	
SIGNER		SIGNER	SIGNER		SIGNER	
47 Microsoft Dynamic Code Publisher	1	27 Microsoft Corporation (Europe)	19 Microsoft	0	17 Microsoft Windows Hardware Abstraction Layer	
SIGNER		SIGNER	SIGNER		SIGNER	
9 Microsoft Update	Ø	8 Microsoft Corporation MSN Ø	7 EventTracker Security LLC	Ø	6 Microsoft Azure Code Sign	
SIGNER		SIGNER	SIGNER		SIGNER	
5 Microsoft LIVE Gaming for Windows	Ø	5 Microsoft Open Technologies Inc	5 Microsoft Windows PE 3	Ø	3 Microsoft Product 2 PE Signing 1	
	0	SIGNIER	SIGNED	0	CIGNER	



### 7.1.4 Approved Collection

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

≡	Nétsurion., EventTracker			• •
	Processes			♠ / EventTrackerEDR / Processes
<u>⊚</u> !	Vendors: 2,270	G Collection 2 🙂 Approved Ven	dors 30	Overview
		OBSERVED VENDORS COLLECTION APPROV	D VENDORS APPROVED COLLECTION IMPORT EXPORT	Processes
	Search Approved Vendor Name	Ø,		
	Testing	Ø		2,097,459 Denied
	Process Count	3,376		
	Vendor Count	16		RESEARCH 1
	Page Size 50 • (1	of 1 GO >		
	⊕ Rules: 3	✓ Allowed 2 × Denied 1		
	+ Allowed Process: 2,097,459			
	Denied Process: 1			
	Research Process: 1			

#### Figure 53

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

OBSERVED VENDORS	DILECTION APPROVED VENDORS APPROVED COLLECTION IMPORT EXPORT	Processes
Arch Collection Nar     Q     Q       Testing Collection1     Image: Collection 1     Image: Collection 1       Process Count     117       Vendor Count     Image: Collection 1	+ Create New Si Testing Collection2 © 1 Process Count 2.024 Vendor Count 3	igner Collection

Figure 54

 $\geq$ 

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

S Allow Vendor Collection	×
Global 🕲	Select Group <b>9</b>
	Approve
Fig	ure 55

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

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

## Allow Vendor Collection

Global 🐼	Select Group 🛛
vailable Groups	Selected Groups
Refine Search	Refine Search
NTPL Win 7 and Server 2008 Above Win XP and Server 2003 Domain Controllers Firewall Devices Network Devices VmWare EventTracker Default A2B After Dark Airlines Allensolly AmericanExpress	Image: Normal state of the



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

-							
D	ro	-		~	~	0	<b>C</b>
<b>_</b>	IU	U	e		э	e	э.
		~	-	-	-	~	-

□ Vendors: 2,265	😼 Collection 2 🙂 A	pproved Vendor	s 30			
	OBSERVED VENDORS	COLLECTION	APPROVED VENDORS	APPROVED COLLECTION	IMPORT	EXPORT
Search Approved Vendor Name 🔍 🔍						
Testing	Ø					
Process Count	3,376					
Vendor Count	16					
🗹 Disallow						



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

#### 7.1.5 Import Vendors

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

Import Vendors		×
Test vendor file.txt		🖙 Browse
Note: Please select file of type *.txt.		
Signer O Product		
		Import Vendors
	Figure 58	

### 7.1.6 Export Vendors

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



## 7.2 Rules

1. Click  $\textcircled{}^{\oplus}$  icon to expand the Rules tab.



Figure 60

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

□ Rules: 4	✓ Allowed Rules	2 × Denied Rules 2		
		ALLOWED RULES DE	NIED RULES	
Search Allowed Rule Names	Q. Q.			+ New Allowed Rule
C://shakti/test/folder	Ø Î	Test	Ø II	
Page Size 25 V C 1	of 1 GO >			

Figure 61

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

Search Allowed Rule Names Q Q A	
Search Allowed Rule Names Q Q + Ne	
	ew Allowed Rule
C://shakti/test/folder 🧭 🗓 Test 🗭 🗓	
Page Size 25 V ( 1 of 1 GO )	



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

Add Rule	×
Rule	
C-\WINDOWS\System32\wups.dll	
Allow Child process	
Note: Rule will be allowed at global level, for more setting please visit process dashboard	
	Add Close





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

Processes			
🗄 Vendors: 5	g Collections 2		
Rules: 4	✓ Allowed Rules 2 × Denied Rules 2		
Search Denied Rule Names	ALLOWED RU	LES DENIED RULES	+ New Denied Rule
D://test/shakti/sample	Ø         Ĩ         F://testing/test           of         1         GO         >	Ø Î	



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

Add Rule	×
Rule	
C-\WINDOWS\System32\wups.dll	
Allow Child process	
Note: Rule will be denied at global level, for more setting please visit process dashboard	
	Add
	Close

#### Figure 65

### 7.3 Allowed Process

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

#### Figure 66

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



□ Allowed Process: 2,097,459

Search	'Hash' or 'File I 🔍 🔍			
	File Name	Opinion	Places	
(+)	wuaueng.dll	UNKNOWN	2	:
+	appraiser.dll	UNKNOWN	2	:
(+)	microsoft.sqlserver.configuration.rsextension.resources.dll	SAFE	0	:
+	microsoft.sqlserver.configuration.resources.dll	SAFE	0	:
$(\pm)$	microsoft.sqlserver.configuration.repl_configextension.resources.dll	SAFE	0	:

#### Figure 67

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

	Allowed Process: 2,097,459				
Searc	h 'Hash' or 'File I 🔍 🔍				
	File Name	Opinion	Places		
÷	wuaueng.dll	UNKNOWN	2	:	
+	appraiser.dll	UNKNOWN	2	:	
+	microsoft.sqlserver.configuration.rsextension.resources.dll	SAFE	0	:	
+	microsoft.sqlserver.configuration.resources.dll	SAFE	0	÷	
+	microsoft.sqlserver.configuration.repl_configextension.resources.dll	SAFE	0	:	

#### Figure 68

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



Allowed Process: 2,097,459

File Name					Opinion	Places	
wuaueng.dll					UNKNOWN	2	
File Name wuaueng.dll					File names found		1
File Version	10.0.17134.1				wuaueng.dll		
Product Name	Microsoft® Windo	ws® Operating Sy	ystem				
Signed By	N/A						
Counter Signed By	N/A						
Signed On							
File Modified Time	Jul 18 09:16:39 AM						
File Path	C:\Windows\Syster	n32\wuaueng.dll					
MD5 Checksum	_	Hash Opinion	Opinion Reference	VirusTotal Ratio			
1dea4d396ed7c1c895e5	cd13f60ed10d	UNKNOWN		0/0			
VirusTotal Link www.virustotal.com			Threat Engine: <u>IBM XF</u>	<u> Malc0de Team Cymru</u>			

Figure 69

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

File Name					Oninian	( All
File Name					Upinion	✓ Allow
wuaueng.dli					UNKNOWN	× Deny
File Name					File names found	
wuaueng.dll					wuaueng.dll	
File Version	10.0.17134.1					
Product Name	Microsoft® Windo	ws® Operating Sys	tem			
Signed By	N/A					
Counter Signed By	N/A					
Signed On						
File Modified Time	Jul 18 09:16:39 AM					
File Path	C:\Windows\Syster	n32\wuaueng.dll				
MD5 Checksum		Hash Opinion	Opinion Reference	VirusTotal Ratio		

Figure 70

### 7.4 Denied Process

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





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

Denied	Process: 1			
Search 'Has	sh' or 'File t 🔍 🍳			
	File Name	Opinion	Places	
+	HashMyFiles.exe	UNKNOWN	1	:
Page Size 2	5 <b>v</b> < 1	of 1 GO >		

Figure 72

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

Denied Process: 1					
Search 'Has	sh' or 'File î 🔍 🔍				
	File Name	Opinion	Places		
÷	HashMyFiles.exe	UNKNOWN	1	:	
Page Size 2	5 ▼ < 1	of 1 GO >			



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





File N	ame		Opinion		Places	
HashN	/yFiles.exe		UNKNOWN		1	
File Name HashMyFilos ovo					File names found	1
File Version	1.70				HashMyFiles.exe	
Product Name	HashMyFiles					
Signed By	N/A					
Counter Signed By	N/A					
Signed On						
File Modified Time	Jul 18 11:00:35 AN	1				
File Path C:\Users\chethan\Desktop\HashMyFiles.exe		iles.exe				
MD5 Checksum	2405065-2226h 🗍	Hash Opinion	Opinion Reference	VirusTotal Ratio		
6611C98da38450d1006	3495965833260	UNKINOWIN		0/0		
www.virustotal.com			Threat Engine: <u>IBM XFE</u>	Malc0de Team Cymru		

Figure 74

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

Denied Process: 1						
earch 'Hash' or 'File   🔍						
File Nar	ne		Opinion		Places	
HashMy	Files.exe		UNKNOWN		1	[
File Name HashMyFiles.exe					File names found	1
File Version	1.70				HashMyFiles.exe	
Product Name	HashMyFiles					
Signed By	N/A					
Counter Signed By	N/A					
Signed On						
File Modified Time	Jul 18 11:00:35 AM					
File Path C:\Users\chethan\Desktop\HashMyFiles.		iles.exe				
MD5 Checksum 661fc98da38450df00684	95965a3326b	Hash Opinion UNKNOWN	Opinion Reference	VirusTotal Ratio 0/0		
VirusTotal Link www.virustotal.com			Threat Engine: IBM XFE	<u>Malc0de Team Cymru</u>		

Figure 75

### 7.5 Research Process

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

<sup>E</sup> Vendors: 66,270	🕢 Collections 4 🙂 Approved Vendors 34
Rules:	✓ Allowed Rules 0 × Denied Rules 0
Allowed Process: 2,097,495	
Denied Process: 2	
Research Process: 3	



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

Rese	earch Process: 1			
Search	'Hash' or 'File t 🔍 🔍			
	File Name	Opinion	Places	
+	softokn3.dll	UNKNOWN	1	:
Page Size	25 🔻 < 1	of 1 GO >		

Figure 77

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

$\exists$ Research Process: 1			
Search 'Hash' or 'File t			
File Name	Opinion	Places	
🛨 softokn3.dll	UNKNOWN	1	:
Page Size 25 V ( 1 of	GO		

Figure 78

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



earch 'Hash' or 'File	Q Q					
File	Name	Орі	nion		Places	
) sof	tokn3.dll	UNI	KNOWN		1	
File Name softokn3.dll					File names found	
File Version	68.0				softokn3.dll	
Product Name	Firefox					
Signed By	Mozilla Corporatio	'n				
Counter Signed By	Symantec Time Sta	amping Services Sign	er - G4			
Signed On						
File Modified Time	Jul 18 07:12:36 AN	1				
File Path C:\Program Files\Mozilla Firefox		1ozilla Firefox∖softok	n3.dll			
MD5 Checksum	22be29b5dbbd67	Hash Opinion	Opinion Reference	VirusTotal Ratio		
VinueTatal Link		0		0,0		

Figure 79

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

arch 'Hash' or 'File I	Q. Q.				
File	Name	Opinion		Places	
soft	tokn3.dll	UNKNOWN		1	:
File Name				File names found	1
File Version	68.0			softokn3.dll	
Product Name	Firefox				
Signed By	Mozilla Corporation				
Counter Signed By	Symantec Time Stan	nping Services Signer - G4			
Signed On					
File Modified Time	Jul 18 07:12:36 AM				
File Path	C:\Program Files\Mo	ozilla Firefox\softokn3.dll			
MD5 Checksum d1e6daa0fda0cf28d48	32be29b5dbbd67	Hash Opinion Opinion Reference	VirusTotal Ratio 0/0		
VirusTotal Link www.virustotal.com		Threat Engine: IBM X	FE <u>Malc0de Team Cymru</u>		

Figure 80

**Netsurion**<sub>•</sub> | EventTracker<sup>•</sup>

## 8. Sensors page

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

Ne Ne	é <b>tsurion.</b> EventTrack	er						
≕ Se	ensors							♠ / EventTrackerEDR / Sensor
•	Sensors: 5	a <sup>™</sup> B Groups: 147	Search 'Group Name'			Q Q	Overview	
		Group	Sensors on Location	State	Mode		Sensor Mode	
	÷	Win 7 and Server 2008 Above	0	000	0000	1	LOCKDOWN	
	÷	Win XP and Server 2003	0	000	0000	÷		U
	+	Domain Controllers	0	000	0000	I	CRITICAL	2
	+	Firewall Devices	0	000	0000	1	HIGH	6
	+	Network Devices	0	000	0000	I		3
	÷	VmWare	0	0 0 0	0000	÷	GUARDED	0
	+	EventTracker	1	0 0 1 0	0010	i.		0
	+	Default	4	1000	0 2 2 0	E.	Sansor Stata	
	÷	NTPL	4	1 1 3 0	0 2 2 0	1	ALERTING	
	+	Test Group	0	0000	0000	i.		1
	+	Sample	0	0000	0000	1	NON REPORTING	0
	+	A2B	0	0000	0000	1		1
	+	After Dark	0	0000	0000	1	AUDIT	6
	+	Airlines	0	0000	0000	1		5
	+	Allensolly	0	0000	0000	1	TERMINATE	0
	+	AmericanExpress	0	0000	0000	1		0
	÷	Armani	٥	000	0000	:		
	+	Arsenal	0	0000	00		1 3 A /* 1	

Figure 81

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

Color	Mode
Red	Lockdown
Orange	Critical
Yellow	High
Blue	Guarded





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

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

Sensors					
Sensors: 6	∎ <sup>®</sup> ∎ Groups: 147	Search 'Group Name'			Q Q
	Group	Sensors on Location	State	Mode	
÷	Win 7 and Server 2008 Above	0	0 0 0	0000	1
÷	Win XP and Server 2003	0	000	0000	÷
÷	Domain Controllers	0	000	000	1
÷	Firewall Devices	0	000	0000	1
÷	Network Devices	0	000	000	÷
÷	VmWare	0	000	0000	1
÷	EventTracker	1	0 0 1 0	0010	1
÷	Default	5	0000	0020	÷
+	NTPL	4	000	0121	1

Figure 82

4. Click the tools option <sup>‡</sup>, to change the **Group Mode** and the action.

6									
					'Group Name'	Se	📲 Groups: 147		Sensors: 5
Mode		Mode	State	s on Location	Sensor			Group	
LockDown	0	000	0000	0			2008 Above	Win 7 and Serve	+
Critical	0	000	0000	0			er 2003	Win XP and Sen	+
High	0	000	0000	0			ers	Domain Control	+
Guarded	0	000	0000	0				Firewall Devices	+
Action	0	000	0000	0				Network Device	+
Terminatr	0	000	000	0				VmWare	+
Contact Info	0	001	0000	1				EventTracker	+
Edit Group I	2 0	0 2 2	2040	4				Default	Ξ
				Secondary Phone	Secondary Email	Secondary Cor	Primary Email Primary Phone	Primary Contact r Name'	Group Address Search 'Sensor
	Action	Mode	Last Check In		alled	Date	IP Address	ter	Comput
	Audit	High	Apr 04 12:10:35 PM				192.168.198.1	BLR33	NTPLDT
	Audit	Critical	Mar 02 11:50:18 AM		:09:23 AM	Jun	172.28.9.153	M9	R1S5-VM
	Audit	High	Apr 04 11:13:07 AM		:35:28 AM	Apr	172.28.100.24	BLR81	NTPLDT
	Audit	Critical	Apr 04 12:07:47 PM		:23:33 AM	Mar	172.28.9.144	M1	R1S5-VM

Figure 83

### 8.1 Edit Group Info

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

Click Edit Group Info to open the Edit Group window.

Mode					
LockDown					
Critical					
High					
Guarded					
Action					
Audit					
Terminate					
Contact Info					
Edit Group Info					
Figure 84					

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



Edit Group		×
GROUP IDENTIFICATION Group Name		
Win 7 and Server 2008 Above		
LOCATION / ADDRESS Address1		
Address2		
Zip		
State		
Country		
CONTACT INFO Primary Contact Name		
Secondary Contact Name		
Primary Contact		
Secondary Contact		
Primary Email		
Secondary Email		
	Close	Update Group

Figure 85

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

Sensors					
Sensors	5: 5 B <sup>B</sup> B Groups: 147	Search 'Group Name'			Q Q
	Group	Sensors on Location	State	Mode	
÷	Win 7 and Server 2008 Above	0	0 0 0 0	0000	1
+	Win XP and Server 2003	0	0 0 0	0000	1
÷	Domain Controllers	0	000	0000	1
+	Firewall Devices	0	000	0000	1
+	Network Devices	0	000	0000	1
+	VmWare	0	0000	0000	1
+	EventTracker	1	1010	0 1 0 0	1
+	Default	4	1 3 2 2	0 1 2 1	1
+	NTPL	2	1011	0 1 1 0	1
+	A2B	0	0 0 0 0	0000	÷

#### Figure 86

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

- NTPL			4	1 0 0	0 2 2	0	
Group Address Primary Contact Search 'Sensor Name'	Primary Email Primary Phone	Secondary Contact Secondary Email	Secondary Phone				
Computer	IP Address	Date Installed		Last Check In	Mode	Action	
NTPLDTBLR33	192.168.198.1			Apr 04 02:28:54 PM	High	Audit	1
R1S5-VM9	172.28.9.153	Jun 03 10:09:23 AM		Mar 02 11:50:18 AM	Critical	Audit	1
NTPLDTBLR81	172.28.100.24	Apr 04 08:35:28 AM		Apr 04 11:13:07 AM	High	Audit	1
R1S5-VM1	172.28.9.144	Mar 04 11:23:33 AM		Apr 04 02:27:00 PM	Critical	Audit	1

#### Figure 87

3. The user can click **tools option**<sup>1</sup>, to change the Sensor **Mode** and **Action**.

į	- NTPL			4	1000	002	0		- 1
	Group Address Primary Contact Search 'Sensor Name'	Primary Email Primary Phone	Secondary Contact Secondary Ernal	Secondary Phone					
	Computer	IP Address	Date Installed		Last Check In	Mode	Action	Mode	
	NTPLDTBLR33	192.168.198.1			Apr 04 02:28:54 PM	High	Audit	LockDown	
	R155-VM9	172.28.9.153	Jun 03 10:09:23 AM		Mar 02 11:50:18 AM	Critical	Audit	Critical	I.
	NTPLDTBLR81	172.28.100.24	Apr 04 08:35:28 AM		Apr 04 11:13:07 AM	High	Audit	High	1
	R155-VM1	172.28.9.144	Mar 04 11:23:33 AM		Apr 04 02:27:00 PM	Critical	Audit	Guarded	I.
								Action	
								Audit	
								Terminate	
								Contact Info	
								Edit Sensor Info	

Figure 88

ange Sensor Mode		
System Name		
NTPLDTBLR301		
SENSOR MODE O Lockdown O Critical   High O Guarded		
SENSOR ACTION Audit O Terminate  Allow All Signed Process		
	Close Up	date Sensor Moo

Figure 89

## 8.2 Edit Sensor Info

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

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



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



×

_		~		
100				
		-		
_		-		

SENSOR IDENTIFICATION System Name	
NTPLDTBLR31~SECURITY	
LOCATION / ADDRESS	
Address1	
bangalore	
Address2	
bangalore	
City	
Bengaluru	
Zip	
560049	
r	
Secondary Contact Name	
Primary Contact	
1321345456	
Secondary Contact	
121231213	
Primary Email	
Det.com	
Secondary Email	
Pet.com	
	Close Lindate Sensor

Figure 91





## 9. Agent Resource Utilization

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

Agent CPU usage: 15% to 20%.

Agent Memory usage: 430MB to 450MB.

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



