EventTracker:

Actionable Security Intelligence

Integrate Bitdefender GravityZone

EventTracker v9.x and above

Publication Date: June 27, 2018

Abstract

This guide provides instructions to configure a **Bitdefender GravityZone** to send its syslog to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version v9.x or above and Bitdefender GravityZone.

Audience

Administrators who are assigned the task to monitor Bitdefender GravityZone events using EventTracker.

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

This document is for informational purposes only. EventTracker 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 EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker 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 EventTracker, 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.

© 2018 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



Table of Contents

Abstract	1
Scope	1
Audience	1
Overview	3
Prerequisites	3
Integration of Bitdefender GravityZone with EventTracker Manager Configuring Log Delivery	3 3
EventTracker Knowledge Pack Categories	7 7
Knowledge Objects	8
Flex Reports	9
Import Bitdefender GravityZone knowledge pack into EventTracker	L8 L9
Knowledge Objects	20
Flex Reports	22
Dashlets	24
Verify Bitdefender GravityZone knowledge pack in EventTracker	26 26
Knowledge Objects	26
Flex Reports	27
Sample Flex Dashboards	28



Overview

Bitdefender GravityZone is the new Bitdefender enterprise security solution for Medium to Very Large Organizations. GravityZone leverages Bitdefender's acclaimed antimalware technologies and provides a centralized security management platform for physical, virtualized and mobile endpoints.

EventTracker helps to monitor events from Bitdefender GravityZone. Its knowledge objects and flex reports will help you to analyze firewall, device control, threat and phishing related details.

Prerequisites

- EventTracker v9.x or above should be installed.
- Bitdefender GravityZone Elite Security or Bitdefender GravityZone Business Security Cloud should be configured for forwarding logs.

Integration of Bitdefender GravityZone with EventTracker Manager

Configuring Log Delivery

To configure a Bitdefender GravityZone to forward logs to an EventTracker server, follow the below steps:

Generate API Key

The API key is a unique key that is generated in My Account section of Bitdefender Control Center.

To generate API keys:

- 1. Log in to https://YOUR-HOSTNAME/ using your administrative account. Your account must have the following rights: Manage Networks, Manage Users, Manage Company and Manage Reports.
- 2. Click your **username** in the upper-right corner of the console and choose **My Account** as shown in the below image.



Integrate Bitdefender Gravityzone





- 3. Go to the **API key section** and click the **Add** button at the upper side of the table.
- 4. Checkbox the APIs that you want to use.

API key			×
Enabled APIs:	Packages API Network API	Policies API	
Save	Cancel		



5. Under Control Center API, Copy the Access URL

Control Center API	
Access URL:	https://cloud.gravityzone.bitdefender.com/api



Bitdefender Integrator

- The **Bitdefender** integrator package needs to be obtained from the EventTracker support team.
- The Integrator package will be obtained in a Zip file format. Extract the files to get the below contents as shown in the figure.



Name	Date modified	Туре	Size
🖶 BitDefender Integrator.exe	06/22/2018 11:45	Application	74 KB
🔁 BitDefender Integrator.exe.config	06/22/2018 11:45	XML Configuratio	1 KB
🚯 BitDefender Reports.csv	05/23/2018 7:24 PM	Microsoft Excel C	1 KB
🔁 Report-BitDefender.exe	06/18/2018 2:31 PM	Application	57 KB
🔁 Report-BitDefender.exe.config	06/18/2018 2:31 PM	XML Configuratio	1 KB

- Right-click on the **Bitdefender Integrator.exe** and **run as administrator** to start the integration process.
- Once you click the .exe, you will get a pop up window as shown in below figure:

💀 Bitdefender Integrator	_		×
Powershell 5.0	In	stall	
EventTracker Agent/Manager	In	stall	
Nev	+	Cancel	1
		Calicer	
Figure 5			h

- Pre-request for integration is if the system contains both PowerShell 5.0 and Eventtracker Agent installed only then you can proceed to the next window by clicking on next. If it is not present you will not be able to proceed till the pre-requisite is met as shown in the above image.
- Provide the Bit defender zone **activity URL** and **API Key** which was obtained from the previous steps as shown in Figure 3.



🖳 Bitdefender Integrator	- 🗆 X	
Bit Defender URL	ne.bitdefender.com	
Bit Defender API Key	13FSUpJnh5jzhf+9H	
Get	Companies	
	Ok Cancel	
		/



• Once URL and API key entered to select the **company** from the list appeared as shown below.

🖳 Bitdefender Integrator	_		
Bit Defender URL	ne.bitdefend	er.com	[
Bit Defender API Key	13FSUpJnh5j	izhf+9h	
Get (Companies		
Netsurion technolo	gies pvt. Itd.		
l	Ok	Ca	incel

Figure 7

• Click OK.



• Provide the administrator username and password of the local machine to configure the task scheduler.

Connect to		?	×				
		AF					
Connecting to							
User name:	1		×				
Password:							
	OK	Can	cel				
Figure 8							

• Once configuration is done successfully a message box will appear as shown below.

🖶 Bitdefende	-	×
Configured Success	sfully	
0	К	
Fi	gure 9	

EventTracker Knowledge Pack

Once logs are received by EventTracker manager, knowledge packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Bitdefender GravityZone.

Categories

- **Bitdefender GravityZone: Application Firewall-**This category provides information related to the application which was blocked from connecting to the network based on the rule configured.
- **Bitdefender GravityZone: Antiphishing Activity** -This category provides information related to the Phishing activity that has been detected and blocked at the endpoints.
- **Bitdefender GravityZone: Blocked Applications** This category provides information related to the blocked application and its attributes.
- **Bitdefender GravityZone: Blocked Website Details-** This category provides information related to the blocked websites, source endpoints and the reason for blocked details.



- **Bitdefender GravityZone: Data Protection Email-** This category provides information related to the blocked email sender or recipient by data protection module and rule details which was applied.
- **Bitdefender GravityZone: Data Protection Web-** This category provides information related to the blocked websites by data protection module and rule details which was applied.
- **Bitdefender GravityZone: Device Control Activity-** This category provides information related to the devices which are allowed or blocked at the endpoints and its attributes.
- **Bitdefender GravityZone: Firewall Activity-** This category provides information related to the IP address or port which were blocked by the Bitdefender based on the rule configured.
- **Bitdefender GravityZone: Malware Activity-** This category provides information related to the threat which was detected at the endpoints and its attributes.
- **Bitdefender GravityZone: Malware Status** This category provides information related to the status of the threat that was detected.
- **Bitdefender GravityZone: On-Demand Scan Details-** This category provides information related to the on-demand scanning details and results.
- **Bitdefender GravityZone: Security Audit-** This category provides information related to the security events from different modules which were occurred.

Knowledge Objects

- **Bitdefender GravityZone Antiphishing Activity-** This knowledge object will help us to analyze logs related to Phishing activity that has been detected and blocked at the endpoints.
- **Bitdefender GravityZone Application Firewall** This knowledge object will help us to analyze logs related to the application which were blocked from connecting to the network, based on the rule configured.
- **Bitdefender GravityZone Blocked Applications** This knowledge object will help us to analyze logs related to the blocked application and its attributes.
- **Bitdefender GravityZone Blocked Website Details** This knowledge object will help us to analyze logs related to the blocked websites, source endpoints and the reason for blocked activity.
- **Bitdefender GravityZone Data Protection Email-** This knowledge object will help us to analyze logs related to the blocked sender or recipient email by data protection module and rule details which was applied.



- **Bitdefender GravityZone Data Protection Web** This knowledge object will help us to analyze logs related to the blocked websites by data protection module and rule details which was applied.
- **Bitdefender GravityZone Device Control Activity-** This knowledge object will help us to analyze logs related to the device which were allowed or blocked in endpoints and its attributes.
- **Bitdefender GravityZone Firewall Activity-** This knowledge object will help us to analyze logs related to the IP address or port which were blocked by the Bitdefender based on the rule configured.
- **Bitdefender GravityZone Malware Activity** This knowledge object will help us to analyze logs related to the threat which were detected at the endpoints and its attributes.
- **Bitdefender GravityZone Malware Status** This knowledge object will help us to analyze logs related to the status of the threat that was detected.
- **Bitdefender GravityZone On-Demand Scan Details-** This knowledge object will help us to analyze logs related to the on-demand scanning details and results.
- **Bitdefender GravityZone Security Audit-** This knowledge object will help us to analyze logs related to the security events from different modules which were audited.

Flex Reports

• **Bitdefender GravityZone** - **Antiphishing Activity** – This report gives the information about Phishing activity that has been detected and blocked at the endpoints.

								Number of blocked		
LogTir	ne	Computer	Company Name	User Name	Endpoint FQDN	Endpoint Name	Last Blocked	attempts	Url	Туре
06/18/2	018 12:20:25 PM	NTPLDTBLR47	contoso systems	williams	contoso-sys1	contoso-sys1	13 June 2018, 16:38:00	12	http://chaina.d148.5kweb.cn/Ong ai.htm	banking
06/18/2	018 12:20:25 PM	NTPLDTBLR47	contoso systems	morris	contoso-pdcsvr3	contoso-pdcsvr3	14 June 2018, 16:38:00	1	http://www.aubchina.cn	banking
06/18/2	018 12:20:25 PM	NTPLDTBLR47	contoso systems	Anderson	contoso-filesvr6	contoso-filesvr6	13 June 2018, 16:38:00	5	http://www.aobchina.cn	banking
06/18/2	018 12:29:35 PM	NTPLDTBLR47	contoso systems	williams	contoso-sys1	contoso-sys1	13 June 2018, 16:38:00	12	http://chaina.d148.5kweb.cn/Ong ai.htm	banking
06/18/2	018 12:29:35 PM	NTPLDTBLR47	contoso systems	morris	contoso-pdcsvr3	contoso-pdcsvr3	14 June 2018, 16:38:00	1	http://www.aubchina.cn	banking
06/18/2	018 12:29:35 PM	NTPLDTBLR47	contoso systems	Anderson	contoso-filesvr6	contoso-filesvr6	13 June 2018, 16:38:00	5	http://www.aobchina.cn	banking





Sample logs:

- Jun 25 12:09:36 PM	ENTRY: Endpoint Name : contoso-sys1 Endpoint FQDN : contoso-sys1 Url : http://chaina.d148.5kweb.cn/Ongai.htm Type : banking User : williams Numbe
event_computer	+- NTPLDTBLR47
event_description	ENTRY:
	Endpoint Name : contoso-sys1
	Endpoint FQDN : contoso-sys1
	Url : http://chaina.d148.5kweb.cn/Ongai.htm
	Type : banking
	User : williams
	Number of blocked attempts : 12
	Last Blocked : 13 June 2018, 16:38:00
	Company Name : contoso systems
	FILE:d\\product\Bit Defender\log sample updated\bitdefenderlog\antiphishing activity.csv
	TYPE:CSV
	FIELD: *

Figure 11

• **Bitdefender GravityZone** - **Blocked application activity** – This report gives the information about the blocked application and its attributes.

	LogTime	Process Name	Path	SHA256 Hash	Endpoint Name	FQDN	User Name	Module		Last Blocked	Company Name
ĺ	06/13/2018 07:20:57 PM	e3ea9ba4-ddd9-49f0-a3fe- cd4dcdec800e.tmp=>eicar.com	C:\Users\Administrator\Downlo ads\e3ea9ba4-ddd9-49f0-a3fe-	275a021bbfb6489e54d471899f7 db9d1663fc695ec2fe2a2c4538	VIN- 68GURACIKUD	win-68guracikud	Administrator	Antimalware	1	13 June 2018, 16:07:13	Contoso systems pvt. ltd.
	06/13/2018 07:20:57 PM	eicar_com (1).zip=>eicar.com	cd4dcdec800e.tmp=>eicar.com C:\Users\Administrator\Downlo ads\eicar_com (1) zin=>eicar.com	aabroolidur N/A	VIN- 68GURACIKUD	win-68guracikud	Administrator	Antimalware	1	13 June 2018, 17:38:18	Contoso systems pvt. ltd.
	06/19/2018 12:29:35 PM	Unconfirmed 73987.crdownload=>eicar.com	C:\Uses\contoso\Downloads\U nconfirmed 73987.crdownload=>eicar.com	275a021bbfb6489e54d471899f7 db9d1663fc695ec2fe2a2c4538 aabf651fd0f	CONTOSO-PC	contoso-pc	contoso	Antimalware	٩	14 June 2018, 15:13:04	Contoso systems pvt. ltd.
	06/18/2018 12:29:35 PM	e799cc83-a245-410c-8153- 55f9257dff64.tmp=>eicar.com	C:\Users\contoso\Downloads\e 799cc83-a245-410c-8153- 55f9257dff64.tmp=>eicar.com	275a021bbfb6489e54d471899f7 db9d1663fc695ec2fe2a2c4538 aabf651fd0f	CONTOSO-PC	contoso-pc	contoso	Antimalware	1	14 June 2018, 15:13:07	Contoso systems pvt. ltd.
ĺ	06/18/2018 12:29:35 PM	calc.exe	C:\Windows\System32\calc.exe	N/A	CONTOSO-PC	contoso-pc	contoso	Content	3	14 June 2018, 15:29:50	Contoso systems pvt. ltd.

Figure 12

Sample logs:

categor checksu event_co event_d

- Jun 25 12:09:36 PM ENTRY: Process : 00b61665-5e3b-4e60-9206-c6a881a1d882.tmp=>eicar.com Path : C\Users\contoso\Downloads\00b61665-5e3b-4e60-9206-c6a881a1d...

/	+- Antimalware
m	+- 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
omputer	+- NTPLDTBLR47
escription	ENTRY:
	Process : 00b61665-5e3b-4e60-9206-c6a881a1d882.tmp=>eicar.com
	Path : C:\Users\contoso\Downloads\00b61665-5e3b-4e60-9206-c6a881a1d882.tmp=>eicar.com
	SHA256 Hash : 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
	Endpoint Name : CONTOSO-PC
	Endpoint FQDN : contoso-pc
	User : contoso
	Module : Antimalware
	Attempts : 1
	Last Blocked : 14 June 2018, 15:13:22
	Company Name : Netsurion technologies pvt. ltd.
	FILE:d:\product\Bit Defender\log sample updated\bitdefenderlog\blocked application activity.csv
	TYPE:CSV
	FIELD: *





• **Bitdefender GravityZone** - **Blocked website activity** – This report gives the information about the blocked websites, source endpoints and the reason for blocked details.

LogTime	Endpoint Name	Endpoint FQDN	Url	Blocked By	Block Reason	User Name	Blocked Attempts	Last Blocked	Company Name
06/14/2018 03:30:58 PM	CONTOSO-PC	contoso-pc	https://www.google.co.in/gen_204	Scheduler	Time constraint	contoso	7	14 June 2018, 14:55:48	Contoso systems pvt. Itd.
06/14/2018 03:30:58 PM	CONTOSO-PC	contoso-pc	https://beacons.gvt2.com/domainreli ability/upload	Scheduler	Time constraint	contoso	14	14 June 2018, 15:00:40	Contoso systems pvt. Itd.
06/14/2018 03:30:58 PM	CONTOSO-PC	contoso-pc	https://www.google.com/chrome/than k-you.html	Control center	malware	williams	1	14 June 2018, 14:57:15	Contoso systems pvt. Itd.
06/14/2018 03:30:58 PM	CONTOSO-PC	contoso-pc	https://www.google.co.in/domainrelia bility/upload	Scheduler	Time constraint	contoso	3	14 June 2018, 14:58:39	Contoso systems pvt. Itd.
06/14/2018 03:30:58 PM	CONTOSO-PC	contoso-pc	https://beacons5.gvt2.com/domainrel iability/upload	Scheduler	Time constraint	contoso	14	14 June 2018, 15:00:46	Contoso systems pvt. Itd.
06/14/2018 03:30:58 PM	CONTOSO-PC	contoso-pc	https://beacons5.gvt3.com/domainrel iability/upload	Scheduler	Time constraint	contoso	14	14 June 2018, 15:00:59	Contoso systems pvt. Itd.
06/14/2018 03:30:58 PM	CONTOSO-PC	contoso-pc	https://beacons4.gvt2.com/domainrel iability/upload	Scheduler	Time constraint	contoso	14	14 June 2018, 15:00:45	Contoso systems pvt. Itd.

Figure 14

Sample logs:

- Jun 25 12:09:36 PM

ENTRY: Endpoint Name : CONTOSO-PC Endpoint FQDN : contoso-pc URL : https://beacons.gvt2.com/domainreliability/upload Blocked By : Scheduler Blo...

event_computer	+- NTPLDTBLR47
event_description	ENTRY:
	Endpoint Name : CONTOSO-PC
	Endpoint FQDN : contoso-pc
	URL : https://beacons.gvt2.com/domainreliability/upload
	Blocked By : Scheduler
	Block Reason : Time constraint
	User : contoso
	Blocked Attempts : 23
	Last Blocked : 14 June 2018, 15:06:39
	Company Name : Netsurion technologies pvt. ltd.
	FILE:d:\product\Bit Defender\log sample updated\bitdefenderlog\blocked website activity.csv
	TYPE:CSV
	FIELD: *

Figure 15

• **Bitdefender GravityZone** - **Data protection web activity** – This report gives the information about the blocked websites by data protection module and rule details which was applied.

LogTime	Endpoint Name	Endpoint FQDN	Website	Rule name	User Name	Number of blocked attempts	Last Blocked	Company Name
06/15/2018 04:04:27 PM	Contoso-pc	contoso-pc	https://www.google.co.in/gen_204	dap-rule	williams	5	14 June 2018, 15:06:36	contoso systems
06/15/2018 04:04:27 PM	Contoso2-pc	contoso2-pc	https://www.google.com/chrome/thank-you.html	dap-rule	williams	5	14 June 2018, 15:06:36	contoso systems
06/15/2018 04:04:27 PM	Contoso3-pc	contoso3-pc	https://www.google.co.in/gen_204	dap-rule	williams	6	14 June 2018, 15:06:36	contoso systems



Sample logs:

- Jun 25 12:09:36 PM	ENTRY: Endpoint Name : Contoso-pc Endpoint FQDN : contoso-pc Website : https://www.google.co.in/gen_204 Rule name : dap-rule User : williams Num
event_computer	+- NTPLDTBLR47
event_description	ENTRY:
	Endpoint Name : Contoso-pc
	Endpoint FQDN : contoso-pc
	Website : https://www.google.co.in/gen_204
	Rule name : dap-rule
	User : williams
	Number of Blocked Attempts : 5
	Last Blocked : 14 June 2018, 15:06:36
	Company Name : contoso systems
	FILE:d:\product\Bit Defender\log sample updated\bitdefenderlog\data protection activity.csv
	TYPE:CSV
	FIELD: *

Figure 17

• **Bitdefender GravityZone** - **Data protection email activity** – This report gives the information about the blocked email sender or recipient by data protection module and rule details which was applied.

							Number of		
		Endpoint					blocked		
LogTime	Computer	Name	Endpoint FQDN	Email	Rule name	User Name	attempts	Last Blocked	Company Name
06/15/2018 04:04:27 PM	NTPLDTBLR47	Contoso-pc	Contoso-pc	williams@contosomailsrv.com	dep-rule_n1	williams	3	14 June 2018, 14:52:10	contoso systems
06/15/2018 04:04:27 PM	NTPLDTBLR47	Contoso2-pc	Contoso2-pc	joe@contosomailsrv.com	dep-rule_lk	joe san	2	14 June 2018, 14:52:10	contoso systems
06/15/2018 04:04:27 PM	NTPLDTBLR47	Contoso2-pc	Contoso2-pc	joe@contosomailsrv.com	dep-rule_lk	joe san	2	14 June 2018, 14:52:10	contoso systems

Figure 18

Sample logs:

- Jun 25 12:09:36 PM	Bitdefender GravityZone Data Protection Email
event_computer	+- NTPLDTBLR47
event_description	ENTRY:
	Endpoint Name : Contoso-pc
	Endpoint FQDN : Contoso-pc
	Email : williams@contosomailsrv.com
	Rule name : dep-rule_n1
	User : williams
	Number of Blocked Attempts : 3
	Last Blocked : 14 June 2018, 14:52:10
	Company Name : contoso systems
	FILE:d:\product\Bit Defender\log sample updated\bitdefenderlog\Data Protection email activity.csv
	TYPE:CSV
	FIELD: *



• **Bitdefender GravityZone** - **Device control activity** -This report gives the information about the devices which are allowed or blocked at the endpoints and its attributes.

Time (4/2018 04:44:55 PM 1	Computer NTPLDTBLR47-DLA	Date 14 June 2018, 14:52:10	Endpoint Name CONTOSO-PC	Endpoint FQDN contoso-pc	Username contoso	Status Allowed	Device Name VBOX CD-ROM	Device Class External Storage	Device ID IDE\CDROMVBOX_CD-	Product ID 454545	Vendor ID	Company Name contoso systems pvt. Itd.
									ROM1.0	-		
4/2018 04:44:55 PM 1	NTPLDTBLR47-DLA	14 June 2018, 14:52:10	CONTOSO-PC	contoso-pc	contoso	Blocked	CD-ROM Drive	CDROM Drive	IDE\CDROMVBOX_CD- ROM1.0	₹ 5	5	contoso systems pvt. ltd.
4/2018 04:44:55 PM 1	NTPLDTBLR47-DLA	14 June 2018, 14:52:10	CONTOSO-PC	contoso-pc	contoso	Blocked	CD-ROM Drive	CDROM Drive	&2117B2E5&0&1.0.0 IDE\CDROMVBOX_CD- ROM	4425452 	ъ	contoso systems pvt. Itd.
					F	gure 2	20					
						-						
nple logs	5:											
- Jun 25 12	2:09:36 PM			Bitdefer	der Gravit	/Zone D	evice Control	Activity				
addl_info1		+	- Product ID									
addl_info2		+	- Vendor ID									
category		+	- Device Class	5								
device_id		+	- Device ID									
device_name		+	- Device Nam	e								
event_compu	iter	+	- NTPLDTBLR	47								
event_descrip	otion	EN	ITRY:									
		En	dpoint Name :	Endpoint Nar	ne							
		En	dpoint FQDN :	Endpoint FQ	DN .							
		Us	ername : Userr	name								
		Sta	atus : Status									
		De	evice Name : De	evice Name								
		De	evice Class : De	vice Class								
		De	evice ID : Device	e ID								
		Pro	oduct ID : Prod	uct ID								
		Ve	ndor ID : Vend	or ID								
		Da	ite : Date									
		Co	mpany Name	Company Na	me							
		FIL	.E:d:\product\B	it Defender\lo	g sample (updated	bitdefenderl	og\device con	trol activty.csv			
		TY	PE:CSV									
		FIE	1 D. *									

Figure 21

• **Bitdefender GravityZone** - **Firewall activity** – This report gives the information about the IP address or port which is blocked by the Bitdefender based on the rule configured.

LogTime	Computer	Endpoint Name	Endpoint FQDN	Source lp	Number of blocked attempts	Last Blocked	Company Name
06/15/2018 02:59:46 PM	NTPLDTBLR47	CONTOSO-PC	contoso-pc	10.2.0.15	5	14 June 2018, 15:13:28	contoso systems
06/15/2018 02:59:46 PM	NTPLDTBLR47	CONTOSO-PC	contoso-pc	10.2.0.15	5	14 June 2018, 15:13:28	contoso systems
06/15/2018 02:59:46 PM	NTPLDTBLR47	CONTOSO-PC	contoso-pc	10.2.0.15	5	14 June 2018, 15:13:28	contoso systems



Sample logs:

- Jun 25 12:09:36 PM	Bitdefender GravityZone Firewall Activity
event_computer	+- NTPLDTBLR47
event_description	ENTRY:
	Endpoint Name : CONTOSO-PC
	Endpoint FQDN : contoso-pc
	Source Ip : 10.2.0.15
	Number of Blocked Attempts : 5
	Last Blocked : 14 June 2018, 15:13:28
	Company Name : contoso systems
	FILE:d:\product\Bit Defender\log sample updated\bitdefenderlog\firewall activity.csv
	TYPE:CSV
	FIELD: *

Figure 23

• **Bitdefender GravityZone** - **Application firewall activity** – This report gives the information about the application which was blocked from connecting to the network based on the rule configured.

							blocked		
LogTime	Endpoint Name	Endpoint FQDN	File Path	Port	Protocol	User Name	attempts	Last Blocked	Company Name
06/15/2018 02:59:46 PM	CONTOSO-PC	contoso-pc	C:\Users\contoso\Downloads\2fd9 2a83-f7d3-4e40-8b55- 95445257c59d.tmp	23	SSH	23	5	14 June 2018, 15:13:28	contoso systems
06/15/2018 02:59:46 PM	CONTOSO-PC	contoso-pc	C:\Users\contoso\Downloads\2cdf asd.tmp	22	Telnet	22	5	14 June 2018, 15:13:28	contoso systems

Figure 24

Sample logs:

- Jun 25 12:09:36 PM	Bitdefender GravityZone Application Firewall
event_computer	+- NTPLDTBLR47
event_description	ENTRY:
	Endpoint Name : CONTOSO-PC
	Endpoint FQDN : contoso-pc
	File Path : C:\Users\contoso\Downloads\2cdfasd.tmp
	Port : 22
	Protocol : Telnet
	User : Williams
	Number of blocked attempts : 5
	Last Blocked : 14 June 2018, 15:13:28
	Company Name : contoso systems
	FILE:d:\product\Bit Defender\log sample updated\bitdefenderlog\Firewall Fileblock activity.csv
	TYPE:CSV
	FIELD: *



• **Bitdefender GravityZone** - **Malware activity** – This report gives the information about the threat which was detected at the endpoints and its attributes.

		Endpoint									
LogTime	Computer	Name	Endpoint FQDN	User Name	Malware name	File Path	SHA256 Hash	Status	Count	Last Detection	Company Name
06/15/2018 12:28:50 PM	NTPLDTBLR47	CONTOSO-PC	contoso-pc	contoso	EICAR-Test-File (not a virus)	C:\Users\contoso\Downl oads\2fd92a83-f7d3- 4e40-8b55- 95445257c59d.tmp	275a021bbfb6489 e54d471899f7db9 d1663fc695ec2fe 2a2c4538aabf651 fd0f	Still Infected	1	14 June 2018, 15:13:28	Contoso systemspvt. Itd.
06/15/2018 12:28:50 PM	NTPLDTBLR47	CONTOSO-PC	contoso-pc	contoso	EICAR-Test-File (not a virus)	C:\Users\contoso\Downl oads\Unconfirmed 73987.crdownload=>eic ar.com	275a021bbfb6489 e54d471899f7db9 d1663fc695ec2fe 2a2c4538aabf651 fd0f	Still Infected	1	14 June 2018, 15:13:04	Contoso systemspyt. Itd.
06/15/2018 12:28:50 PM	NTPLDTBLR47	CONTOSO-PC	contoso-pc	contoso	EICAR-Test-File (not a virus)	C:\Users\contoso\Downl oads\dc2325d1-0b95- 4e4c-8751- 4d6663a322b4.tmp	N/A	Still Infected	1	14 June 2018, 15:13:19	Contoso systemspvt. Itd.
06/15/2018 12:28:50 PM	NTPLDTBLR47	CONTOSO-PC	contoso-pc	contoso	EICAR-Test-File (not a virus)	C:\Users\contoso\Downl oads\00b61665-5e3b- 4e60-9206- c6a881a1d882.tmp=>eic ar.com	275a021bbfb6489 e54d471899f7db9 d1663fc695ec2fe 2a2c4538aabf651 fd0f	Resolved	1	14 June 2018, 15:13:22	Contoso systemspyt. Itd.
	LogTime 06/15/2018 12:28:50 PM 06/15/2018 12:28:50 PM 06/15/2018 12:28:50 PM 06/15/2018 12:28:50 PM	LogTime Computer 06/15/2018 12:28:50 PM NTPLDTBLR47 06/15/2018 12:28:50 PM NTPLDTBLR47 06/15/2018 12:28:50 PM NTPLDTBLR47 06/15/2018 12:28:50 PM NTPLDTBLR47	Endpoint Endpoint LogTime Computer Name 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC	Endpoint Endpoint LogTime Computer Name Endpoint F00N 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc	Endpoint Endpoint Endpoint 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso	Endpoint Endpoint FODD User Name Malware name 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus)	LogTime Computer Name Endpoint FQDN User Name Malware name File Path 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C:\Users\contoso\Download\scatege: 494-0.8055- 95445257c59d.tmp 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C:\Users\contoso\Download\scatege: 494-0.8055- 95445257c59d.tmp 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C:\Users\contoso\Download\scatege: 494-0.8055- 95445257c59d.tmp 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C:\Users\contoso\Download\scatege: 494-0.805- 446-8751- 446663322b4.tmp 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C:\Users\contoso\Download\scatege: 496-8751- 446663322b4.tmp 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C:\Users\contoso\Download\scatege: 496-8206- 68881a14882.tmp=>eic ar.com	LogTime Computer Name Endpoint FODN User Name Malware name File Path SHA256 Hash 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C/Users/contoso/Down 275a021bbfb6489 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C/Users/contoso/Down 275a021bbfb6489 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C/Users/contoso/Down 275a021bbfb6489 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C/Users/contoso/Down 275a021bbfb6489 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C/Users/contoso/Down 275a021bbfb6489 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C/Users/contoso/Down 275a021bbfb6489 06/15/2018 12:28:50 PM NTPLDTBLR47	LogTime Computer Name Endpoint FODN User Name Malware name File Path SHA256 Hash Status 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C:\Users\contoso\Down 275a021bbfb6489 Still Infected 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C:\Users\contoso\Down 275a021bbfb6489 Still Infected 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C:\Users\contoso\Down 275a021bbfb6489 Still Infected 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C:\Users\contoso\Down 275a021bbfb6499 Still Infected 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C:\Users\contoso\Down 274c438aabf651 160f 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a v	LogTime Computer Name Endpoint FODN User Name Malware name File Path SHA256 Hash Status Count 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C:\Users\contoso\Down 275a021bbfb6489 Still Infected 1 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C:\Users\contoso\Down 275a021bbfb6489 Still Infected 1 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C:\Users\contoso\Down 275a021bbfb6489 Still Infected 1 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C:\Users\contoso\Down 275a021bbfb6489 Still Infected 1 06/15/2018 12:28:50 PM NTPLDTBLR47 CONTOSO-PC contoso-pc contoso EICAR-Test-File (not a virus) C:\Users\contoso\Down N/A Still Infected 1 06/15/2018 12:28:50 PM NTPLDTBLR47	LogTimeComputerNameEndpoint FQDN User NameMalware nameFile PathSHA256 HashStatusCountLast Detection06/15/2018 12:28:50 PMNTPLDTBLR47CONTOSO-PCcontoso-pccontosoEICAR-Test-File (not a virus)C:\Users\contoso\Down275a021bbfb6489Still Infected114 June 2018, 15:13:2806/15/2018 12:28:50 PMNTPLDTBLR47CONTOSO-PCcontoso-pccontoso-pccontosoEICAR-Test-File (not a virus)C:\Users\contoso\Down275a021bbfb6489Still Infected114 June 2018, 15:13:2806/15/2018 12:28:50 PMNTPLDTBLR47CONTOSO-PCcontoso-pccontosoEICAR-Test-File (not a virus)C:\Users\contoso\Down275a021bbfb6489Still Infected114 June 2018, 15:13:2806/15/2018 12:28:50 PMNTPLDTBLR47CONTOSO-PCcontoso-pccontosoEICAR-Test-File (not a virus)C:\Users\contoso\DownN/AStill Infected114 June 2018, 15:13:0406/15/2018 12:28:50 PMNTPLDTBLR47CONTOSO-PCcontoso-pccontosoEICAR-Test-File (not a virus)C:\Users\contoso\DownN/AStill Infected114 June 2018, 15:13:0406/15/2018 12:28:50 PMNTPLDTBLR47CONTOSO-PCcontoso-pccontoso-pccontosoEICAR-Test-File (not a virus)C:\Users\contoso\DownN/AStill Infected114 June 2018, 15:13:2806/15/2018 12:28:50 PMNTPLDTBLR47CONTOSO-PCcontoso-pccontoso-pccontoso-pccontoso-pccontoso-pcC:\Users\contoso\DownN/ASti

Figure 26

Sample logs:

- Jun 25 12:09:37 PM	Bitdefender GravityZone Malware Activity
checksum	+- 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
event_computer	+- NTPLDTBLR47
event_description	ENTRY:
	Malware name : EICAR-Test-File (not a virus)
	File Path : C:\Users\contoso\Downloads\e7d50fa6-b4bf-4a77-9293-31f854d384c3.tmp
	SHA256 Hash : 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
	Endpoint Name : CONTOSO-PC
	Endpoint FQDN : contoso-pc
	User : contoso
	Status : Resolved
	Last Detection : 14 June 2018, 15:13:28
	Count : 1
	Company Name : Netsurion technologies pvt. Itd.
	FILE:d:\product\Bit Defender\log sample updated\bitdefenderlog\malware activity.csv
	TYPE:CSV
	FIELD: *
	Figure 27

 Bitdefender GravityZone - Malware status – This report gives the information about the status of the threat which was detected.

LogTime	Endpoint Name	Endpoint FQDN	Status	Company Name	User Name	Malware name	Threat Type	File Path	SHA256 Hash	Last Detection
06/15/2018 11:52:28 AM	CONTOSO-PC	contoso-pc	Infected	Netsurion technologies pvt. ltd.	contoso	EICAR-Test-File (not a virus)	Malware	C:\Users\contoso\Downloads\2fd 92a83-f7d3-4e40-8b55- 95445257c59d.tmp	275a021bbfb6489e54d47 1899f7db9d1663fc695ec 2fe2a2c4538aabf651fd0f	14 June 2018, 15:13:28
06/15/2018 11:52:28 AM	CONTOSO-PC	contoso-pc	Infected	Netsurion technologies pvt. ltd.	contoso	EICAR-Test-File (not a virus)	Malware	C:\Users\contoso\Downloads\Unc onfirmed 73987.crdownload=>eicar.com	275a021bbfb6489e54d47 1899f7db9d1663fc695ec 2fe2a2c4538aabf651fd0f	14 June 2018, 15:13:04
06/15/2018 11:52:28 AM	CONTOSO-PC	contoso-pc	Infected	Netsurion technologies pvt. Itd.	contoso	EICAR-Test-File (not a virus)	Malware	C:\Users\contoso\Downloads\dc2 325d1-0b95-4e4c-8751- 4d6663a322b4.tmp	N/A	14 June 2018, 15:13:19
06/15/2018 11:52:28 AM	CONTOSO-PC	contoso-pc	Deleted	Netsurion technologies pvt. ltd.	contoso	EICAR-Test-File (not a virus)	Malware	C:\Users\contoso\Downloads\e79 9cc83-a245-410c-8153- 55f9257dff64.tmp=>eicar.com	275a021bbfb6489e54d47 1899f7db9d1663fc695ec 2fe2a2c4538aabf651fd0f	14 June 2018, 15:13:07
06/15/2018 11:52:28 AM	CONTOSO-PC	contoso-pc	Deleted	Netsurion technologies pvt. Itd.	contoso	EICAR-Test-File (not a virus)	Malware	C:\Users\contoso\Downloads\e7d 50fa6-b4bf-4a77-9293- 31f854d384c3 tmp	275a021bbfb6489e54d47 1899f7db9d1663fc695ec 2fe2a2c4538aabf651fd0f	14 June 2018, 15:13:28



Sample logs :

- Jun 25 12:09:37 PM	Bitdefender GravityZone Malware Status
checksum	+- 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
event_computer	+- NTPLDTBLR47
event_description	ENTRY:
	Endpoint Name : CONTOSO-PC
	Endpoint FQDN : contoso-pc
	Status : Deleted
	Malware name : EICAR-Test-File (not a virus)
	Threat Type : Malware
	User : contoso
	File Path : C:\Users\contoso\Downloads\e7d50fa6-b4bf-4a77-9293-31f854d384c3.tmp
	SHA256 Hash : 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
	Last Detection : 14 June 2018, 15:13:28
	Company Name : Netsurion technologies pvt. ltd.
	FILE:d:\product\Bit Defender\log sample updated\bitdefenderlog\malware status.csv
	TYPE:CSV
	FIELD: *

Figure 29

• **Bitdefender GravityZone** - **On-demand scanning** – This report gives the information about the ondemand scanning details and results.

							Successfu	Failed	Last successful	
LogTime	Computer	Endpoint Name	Endpoint FQDN	Scan Name	Scan Type	Recurrence	Iscans	scans	scan	Company Name
06/15/2018 11:52:28 AM	NTPLDTBLR47	CONTOSO-PC	contoso-pc	Daily scan	Quick Scan	Run every 1 day	1	6	14 June 2018, 16:15:48	Contoso systemspvt. Itd.
06/15/2018 11:52:28 AM	NTPLDTBLR47	CONTOSO-PC	contoso-pc	Week end scan	Quick Scan	Run every 1 week	1	б	14 June 2018, 16:15:48	Contoso systemspvt. Itd.
06/15/2018 11:52:28 AM	NTPLDTBLR47	CONTOSO-PC	contoso-pc	Daily scan	Quick Scan	Run every 1 day	1	б	14 June 2018, 16:15:48	Contoso systemspvt. Itd.
06/15/2018 11:52:28 AM	NTPLDTBLR47	CONTOSO-PC	contoso-pc	Daily scan	Quick Scan	Run every 1 day	1	б	14 June 2018, 16:15:48	Contoso systemspvt. ltd.



Sample logs:

- Jun 25 12:09:37 PM	Bitdefender GravityZone On Demand Scan Details
event_computer	+- NTPLDTBLR47
event_description	ENTRY:
	Endpoint Name : CONTOSO-PC
	Endpoint FQDN : contoso-pc
	Scan Name : My Task
	Scan Type : Quick Scan
	Recurrence : Run every 1 day
	Successful scans : 1
	Failed scans : 0
	Last successful scan : 14 June 2018, 16:15:48
	Company Name : Netsurion technologies pvt. ltd.
	FILE:d:\product\Bit Defender\log sample updated\bitdefenderlog\on demand scanning.csv
	TYPE:CSV
	FIELD: *
	Figure 31

• **Bitdefender GravityZone** - **Security audit** – This report gives the information about the security events from different modules which were audited.

LogTime	Computer	Endpoint Name	Endpoint FQDN	User Name	Occurrences	Module	Event Type	Details	SHA256 Hash	Company Name
06/14/2018 04:44:55 PM	NTPLDTBLR47-DLA	CONTOSO-PC	contoso-pc	contoso	25	Content Control	Blocked Website	Type:Web Control (Scheduler), Website:https://www.google.co.in/ gen_204	N/A	Contoso systems
06/14/2018 04:44:55 PM	NTPLDTBLR47-DLA	CONTOSO-PC	contoso-pc	contoso	3	Content Control	Blocked Application	File Path: C:\Windows\System32\calc.exe	N/A	Contoso systems
06/14/2018 04:44:55 PM	NTPLDTBLR47-DLA	CONTOSO-PC	contoso-pc	contoso	1	Antimalware	Malware Detection	File Path: C:\Users\contoso\Downloads\2fd92 a83-7fd3-4e40-8b55- 95445257c59d.tmp, SHA256 Hash: 275a021bbfb489e5444718997db 9d1663fc695ec2fe2a2c4538aabf65 1d0f, Malware Name: ELCAR-Test-	275a021bbfb6489e54d471 899f7db9d1663fc695ec2fe 2a2c4538aabf651fd0f, Malware Name: ElCAR-Test- File (not a virus), Threat Type: Malware, Status:Blocked	Contoso systems
06/14/2018 04:44:55 PM	NTPLDTBLR47-DLA	CONTOSO-PC	contoso-pc	contoso	٩	Antimalware	Malware Detection	File Path: C:\Users\contoso\Downloads\Unco nfirmed 73987.crdownload=>eicar.com, SHA256 Hash: 275a021bbfb6489e54d471899f7db 9d16637c695ec21e2a2c4538aabf65 fildfi Malywar Name FiCAR-Test.	275a021bbfb6489e54d471 899f7db9d1663fc695ec2fe 2a2c4538aabf651fd0f, Malware Name: ElCAR-Test- File (not a virus), Threat Type: Malware, Status:Blocked	Contoso systems
06/14/2018 04:44:55 PM	NTPLDTBLR47-DLA	CONTOSO-PC	contoso-pc	contoso	4	Antimalware	Malware Detection	File Path: C:\Users\contoso\Downloads\dc23 25d1-0b95-4e4c-8751- 4d6663a322b4.tmp, SHA256 Hash: N/A, Malware Name: EICAR-Test- File (not a virus), Threat Type: Malware, Status:Blocked	N/A, Malware Name: EICAR- Test-File (not a virus), Threat Type: Malware, Status:Blocked	Contoso systems



Sample logs:

- Jun 25 12:09:37 PM	Bitdefender GravityZone Security Audit
category	+- Device Control
checksum	+- N/A
event_computer	+- NTPLDTBLR47
event_description	ENTRY:
	Endpoint Name : CONTOSO-PC
	Endpoint FQDN : contoso-pc
	User : contoso
	Occurrences : 1
	Last Occurrence : 14 June 2018, 14:52:10
	Module : Device Control
	Event Type : Blocked Device
	Details : Device Name: CD-ROM Drive, Device ID: IDE\CDROMVBOX_CD-ROM
	SHA256 Hash : N/A
	Company Name : Netsurion technologies pvt. Itd.
	FILE:d:\product\Bit Defender\log sample updated\bitdefenderlog\security audit.csv
	TYPE:CSV
	FIELD: *

Figure 33

Import Bitdefender GravityZone knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Knowledge Objects
- Flex Reports
- Dash lets
- 1. Launch EventTracker Control Panel.
- 2. Double click Export-Import Utility.





Figure 34

3. Click the **Import** tab.

Category

1. Click **Category** option, and then click the browse button.

Options	Location	
Category		
Filters		
Alerts		
) Systems and Groups	Source :	
) Token Value	D. product tak berender tip teategory_bitderender soar	
) Reports		
Behavior Correlation		





- 2. Locate Category_Bitdefender Gravityzone. iscat file, and then click the Open button.
- 3. To import categories, click the **Import** button.

EventTracker displays a success message.

Export Im	port Utility	×
1	Selected category details are imported successfully.	
	ОК	
	Figure 36	

4. Click **OK**, and then click the **Close** button.

Knowledge Objects

- 1. Click Knowledge objects under Admin option in the EventTracker manager page.
- 2. Locate the file named KO_Bitdefender GravityZone.etko.

Import		×
KO_Bitdefender GravityZone.etko 🖆	Browse Upload	

0	-	-	-
- U	0	15	



3. Now select all the checkbox and then click on 'Import' option.

1	Object name	Applies to	Group name
1	Bitdefender GravityZone Antiphishing Activity	Bitdefender GravityZone	Bitdefender GravityZone
•	Bitdefender GravityZone Application Firewall	Bitdefender GravityZone	Bitdefender GravityZone
1	Bitdefender GravityZone Blocked Applications	Bitdefender GravityZone	Bitdefender GravityZone
•	Bitdefender GravityZone Blocked Website Details	Bitdefender GravityZone	Bitdefender GravityZone
1	Bitdefender GravityZone Data Protection Email	Bitdefender GravityZone	Bitdefender GravityZone
•	Bitdefender GravityZone Data Protection Web	Bitdefender GravityZone	Bitdefender GravityZone
1	Bitdefender GravityZone Device Control Activity	Bitdefender GravityZone	Bitdefender GravityZone
1	Bitdefender GravityZone Firewall Activity	Bitdefender GravityZone	Bitdefender GravityZone
1	Bitdefender GravityZone Malware Activity	Bitdefender GravityZone	Bitdefender GravityZone
•	Bitdefender GravityZone Malware Status	Bitdefender GravityZone	Bitdefender GravityZone
1	Bitdefender GravityZone On Demand Scan Details	Bitdefender GravityZone	Bitdefender GravityZone
•	Bitdefender GravityZone Security Audit	Bitdefender GravityZone	Bitdefender GravityZone

Figure 38

4. Knowledge objects are now imported successfully.





Flex Reports

On EventTracker Control Panel,

1. Click **Reports** option, and select new(etcrx) from the option.

•	Export Import Utility		_		\times
E	xport Import				
	1. Provide the path and file na 2. Click the Import button Note : If report(s) contains tem	me of Schedule Report file. Use the '' button to browse and locate the import file. plate, first import template and proceed with exportimport utility.			
	Options	Location			
	Category				
	O Filters				
	O Alerts	Legacy (*issch) New (*.etcnx)			
	O Systems and Groups	Source :			
	O Token Value	15901			
	Reports				
	O Behavior Correlation				
		Import		Clos	e
		Import		Clos	e

Figure 40

2. Locate the file named **Reports_ Bitdefender GravityZone.etcrx**, and select all the checkbox.



Integrate Bitdefender Gravityzone

vailat	Select file D:\product\Bit Defender\kp\Reports_bitdefender.etcrx Available reports						
itle		Frequency Show all	Q Q				
		Title				Sites	
	EDIT Bitdefender GravityZone - Antiphishing Activity			NTPLDTBLR47			
	EDIT Bitdefender GravityZone - Application firewall activ	vity		NTPLDTBLR47			
\checkmark	EDIT Bitdefender GravityZone - Blocked application act	tivity		NTPLDTBLR47			
	EDIT Bitdefender GravityZone - Blocked website activity	У		NTPLDTBLR47			
$\overline{}$	EDIT Bitdefender GravityZone - Data protection email a	ctivity		NTPLDTBLR47			
	EDIT Bitdefender GravityZone - Data protection web ac	stivity		NTPLDTBLR47			
2	EDIT Bitdefender GravityZone - Device control activty			NTPLDTBLR47			
	EDIT Bitdefender GravityZone - Firewall activity			NTPLDTBLR47			
4	EDIT Bitdefender GravityZone - Malware activity			NTPLDTBLR47			
4	EDIT Bitdefender GravityZone - Malware status			NTPLDTBLR47			
4	EDIT Bitdefender GravityZone - On demand scanning			NTPLDTBLR47			
4	EDIT Bitdefender GravityZone - Security audit			NTPLDTBLR47			
						>	
		and Hourly Reports					
Note	: Set run time option is not applicable for Defined Reports a						
Note Set	: Set run time option is not applicable for Defined Reports run time for report(s) from	at interval of minutes Set	(i)				
Vote Set Rep	: Set run time option is not applicable for Defined Reports run time for report(s) from AM < lace to	at interval of minutes Set	in systems				



3. Click the Import button to import the reports. EventTracker displays a success message.

Export Import Utility	\times
Selected reports configurations are imported successfully	
ОК	





Dashlets

1. Open EventTracker Enterprise in the browser and log in.



Figure 43

- 2. Navigate to **My Dashboard.**
- 3. Click on import configuration \mathbb{F} icon on the top right corner.
- 4. In the popup window browse the file named **Dashboard_Bitdefender Gravityzone.etwd**.





5. Now select all the checkbox and then click on Import option.



Figure 45

6. Click '**customize**' (a) to locate and choose created dashlet.

C	ustomize dashlets			×
	bitdefender			Q
	Bitdefender GravityZone Applic	Bitdefender GravityZone: Blocke	Bitdefender GravityZone: Blocke	Bitdefender GravityZone: Devic
	Bitdefender GravityZone: Firewa	Bitdefender GravityZone: Malwa	Bitdefender GravityZone: Malwa	Bitdefender GravityZone: Securi
				Add Delete Close

Figure 46

7. Click **Add** to add dashlet to the dashboard.



Verify Bitdefender GravityZone knowledge pack in EventTracker

Categories

- 1. Login to EventTracker Enterprise.
- 2. Click Admin drop-down, and then click Categories.
- 3. In **Category Tree** to view imported categories, scroll down and expand Bitdefender GravityZone group folder to view the imported categories.

Category			🕈 / Admin / Category
Category Tree Search	Total category groups: 19 Total categories: 401 Last 10 modified categories		
*All error events	Name	Modified date	Modified by
All information events	MS RRAS: Access Accept	Jun 20 12:06:44 PM	
All warning events	MS RRAS: Accept-Request	Jun 20 12:06:27 PM	
- Security: All security events - Aruba AirWaive	MS RRAS: Request Discard	Jun 20 11:56:10 AM	
P D Aniba OS	MS RRAS: Accounting Type	Jun 20 11:55:46 AM	
Bitdefender GravityZone	MS RRAS: Access Reject	Jun 20 11:55:16 AM	
🗏 Bitdefender GravityZone Application Firewal	MS RRAS: Authentication Failure	Jun 20 11:34:58 AM	
🗐 Bitdefender GravityZone: Antiphishing Activi	Bitdefender GravityZone: Security Audit	Jun 15 06:28:49 PM	
🗐 Bitdefender GravityZone: Blocked Applicatio	Bitdefender GravityZone: On Demand Scan Details	Jun 15 06:27:49 PM	
Bitdefender GravityZone: Blocked Website D	Bitdefender GravityZone: Malware Status	Jun 15 06:26:52 PM	
I Bitdefender GravityZone: Data Protection En	Bitdefender GravityZone: Malware Activity	Jun 15 06:25:56 PM	
Bitdefender GravityZone: Data Protection W			
Bitdefender GravityZone: Device Control Act Bitdefender GravityZone: Firewall Activity			
Bitdefender GravityZone: Malware Activity			
Bitdefender GravityZone: Malware Status			
🗐 Bitdefender GravityZone: On Demand Scan (
Bitdefender GravityZone: Security Audit			

Figure 47

Knowledge Objects

- 1. In the EventTracker Enterprise web interface, click the Admin drop-down, and then click Knowledge Objects.
- 2. In the **Knowledge Object** tree, expand **Bitdefender GravityZone** group folder to view the imported Knowledge objects.



Knowledge Objects						↑ Admin / Knowledge Objects
Search objects	Q Q Activate Now					Objects 🕂 ፒ 🏦 🌣
Groups 🕀 🏈 📋	Object name Bitdefender GravityZone	Antiphishing Activity				🔅 📓 🕼
Apache Web Server	Applies to Bitdefender GravityZone					
Aruba AirWave	Rules					
Aruba OS	Title	Log type	Event source	Event id	Event type	
Bitdefender GravityZone	 Bitdefender GravityZone Antiphis Activity 	ning	bitdefender	3230		Ø 🕑 🗓 🔗
Bitdefender GravityZon 🧭 📋	Message Signature: (?is)Endpoin	t\s+Name.*?Endpoint\s+FQDN	l.*?Url.*?Type.*?User.*?Numbe	r\s+of\s+blocked\s+attempts.*?L	ast\s+Blocked	
Bitdefender GravityZon 🧭 📋	Message Exception:					
Bitdefender GravityZon	Expressions					
Bitdefender GravityZon	Expression type	Express	sion 1	Expression 2	Format string	
Bitdefender GravityZon 🧭 🏢	Key Value Delimiter			\n	2	
Bitdefender GravityZon 🧭 🏢						
Bitdefender GravityZon 🧭 🏢						
Bitdefender GravityZon 🧭 🏢						
Bitdefender GravityZon						
Bitdefender GravityZon						
Bitdefender GravityZon						
		- I	-igure 48			

Flex Reports

1. In the EventTracker Enterprise web interface, click the Reports icon, and then select Report Configuration.



- 2. In Reports Configuration pane, select a Defined option.
- 3. Click on the **Bitdefender GravityZone** group folder to view the imported Bitdefender GravityZone reports.



Report Configuration					† / F	Reports / Report Confi	iguration /	Defined
O Scheduled O Queued Det	fined			Search		Q Q	Ċ	iv
Report Groups	\oplus	Reports con	nfiguration: Bitdefender GravityZone					
[] Security	^	🕀 🗓 d					Total:	12
f: Compliance			Title	Created on	Modified on			
Coperations			Bitdefender GravityZone - Security audit	Jun 14 12:09:09 PM	Jun 15 04:48:21 PM	()	5	+
EB Flex			Bitdefender GravityZone - On demand scanning	Jun 14 12:06:09 PM	Jun 15 04:49:15 PM	()	2	+
All Compliance Repor	Ü 🏈		Bitdefender GravityZone - Malware status	Jun 14 12:01:49 PM	Jun 15 06:35:27 PM	()	5	+
Apache Web Server	1		Bitdefender GravityZone - Malware activity	Jun 14 11:57:30 AM	Jun 15 06:42:29 PM	()	5	+
Aruba AirWave	1		Bitdefender GravityZone - Application firewall activity	Jun 14 11:43:39 AM	Jun 15 04:52:45 PM	()	5	+
ArubaOS			Bitdefender GravityZone - Firewall activity	Jun 14 11:37:13 AM	Jun 15 04:53:19 PM	() ()	2	+
Bitdefender GravityZ			Bitdefender GravityZone - Device control activity	Jun 14 11:28:52 AM	Jun 15 04:54:02 PM	() ()		E
Bluecoat Content Ana			Bitdefender GravityZone - Data protection email activity	lup 14 11:23:45 AM	lup 15 04:54:42 PM	0		
	<u> </u>		Pitelender Gruit-Zene - Data protection eman activity	Jun 14 11/10/25 AM	Jun 15 04:55:45 PM	0		•
Cisco ASA			Bitderender Gravityzone - Data protection web activity	Jun 14 11:18:25 AM	Jun 15 04:55:46 PM	0	0	+
		L \$	Bitdefender GravityZone - Blocked website activity	Jun 14 11:13:40 AM	Jun 15 04:57:34 PM	0	ŏ	+
Microsoft Windows RR								
C Office 365								

Figure 50

Sample Flex Dashboards

Title: Bitdefender GravityZone Application Firewall





Title: Bitdefender GravityZone Blocked Application





Title: Bitdefender GravityZone Blocked Websites



Actionable Security Intelligence

Title: Bitdefender GravityZone Firewall Activity







Title: Bitdefender GravityZone Malware Status





Title: Bitdefender GravityZone Device Control Activity



🖸 – 🗙







Title: Bitdefender GravityZone Security Audit



