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.

# Table of Contents

# 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.

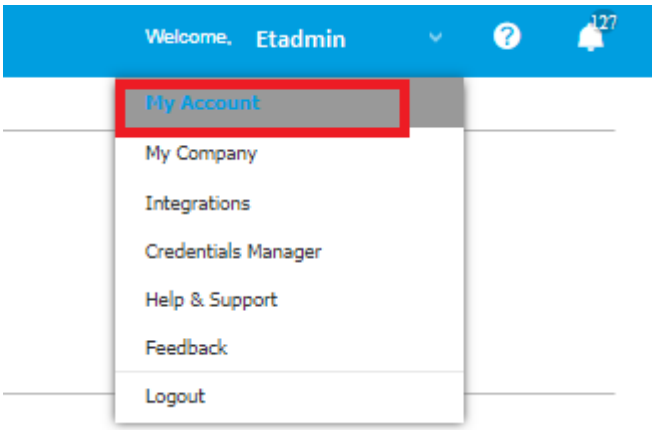


Figure 1

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.

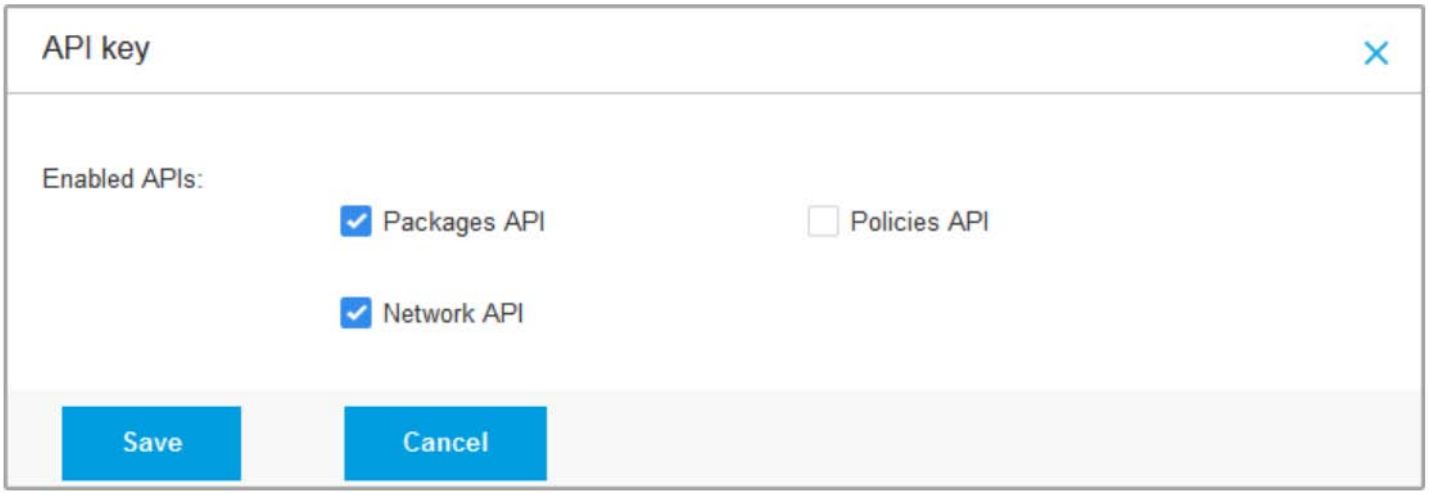


Figure 2

5. Under **Control Center** API, Copy the **Access URL**

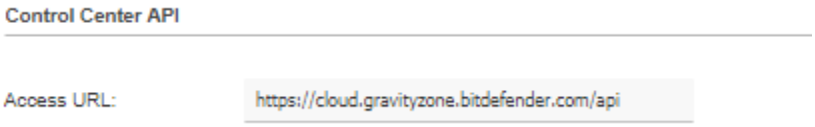


Figure 3

**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 | Type | 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 |

Figure 4

- 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:

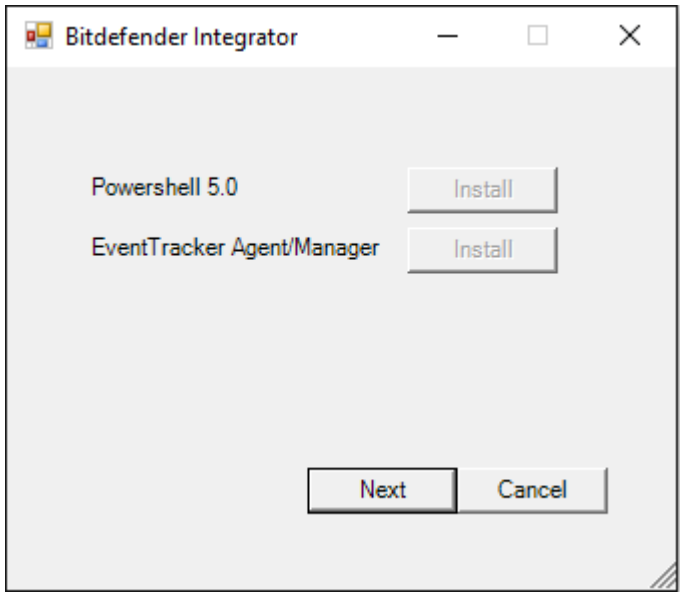


Figure 5

- 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.

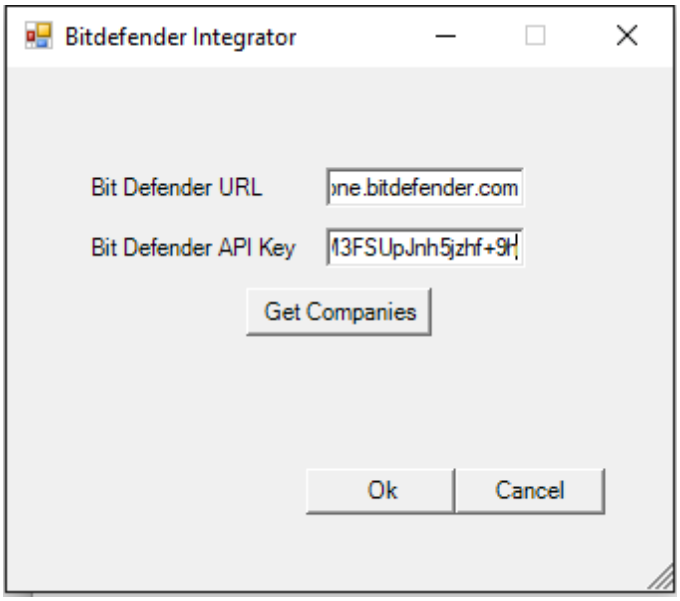


Figure 6

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

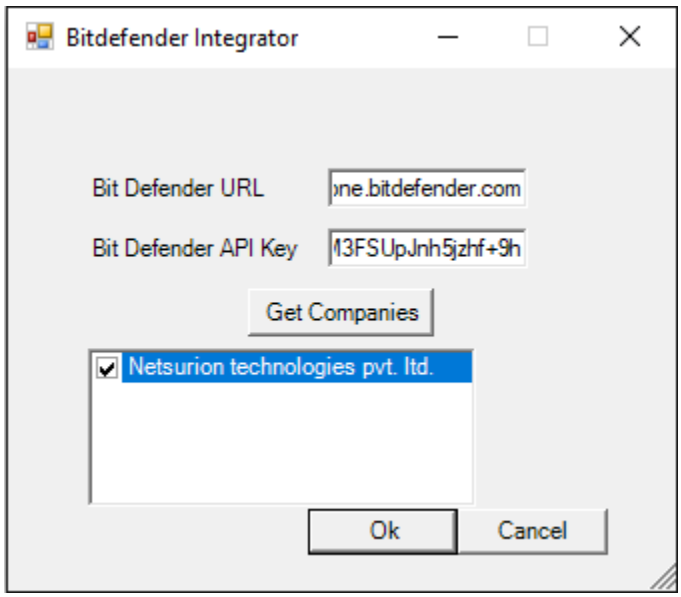


Figure 7

- Click **OK**.

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

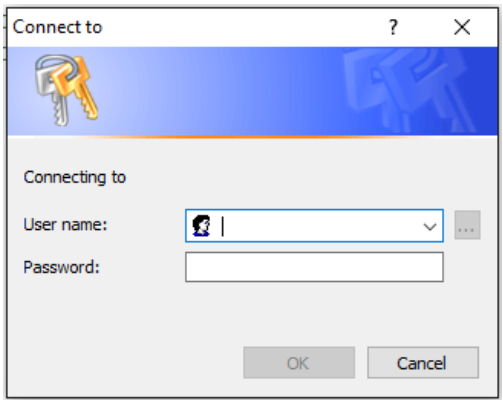


Figure 8

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

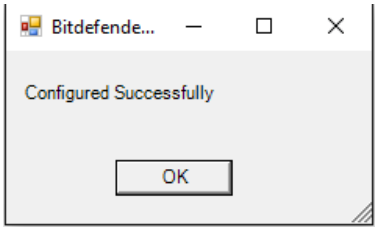


Figure 9

# 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.

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

Figure 10

**Sample logs:**

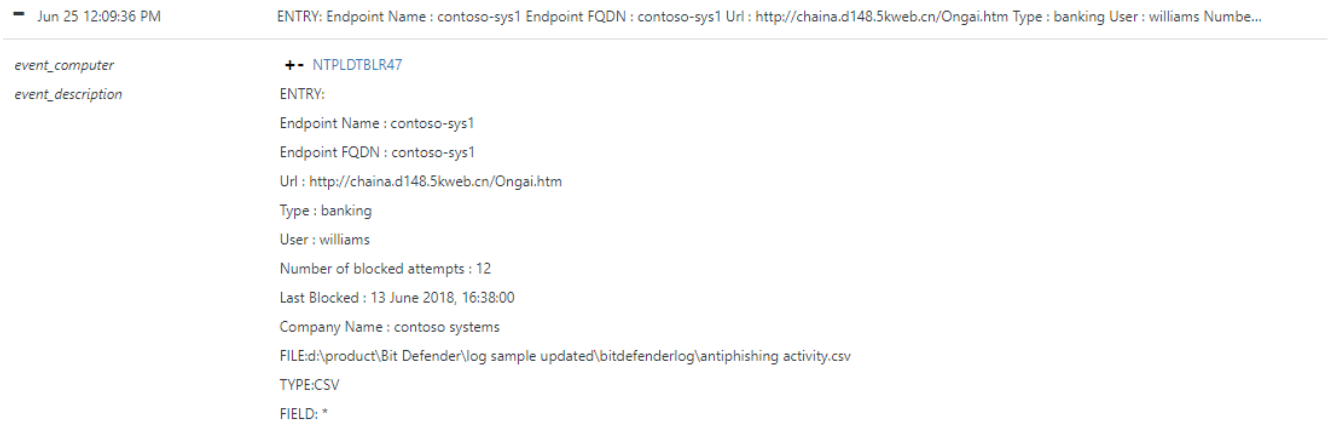


Figure 11

- **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 | s | Last Blocked | Company Name |
|---|---|---|---|---|---|---|---|---|---|---|
| 06/13/2018 07:20:57 PM | e3ea9ba4-ddd9-49f0-a3fe-cd4dcdec800e.tmp=>eicar.com | C:\Users\Administrator\Downloads\e3ea9ba4-ddd9-49f0-a3fe-cd4dcdec800e.tmp=>eicar.com | 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f | WIN-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 | C:\Users\Administrator\Downloads\eicar_com (1).zip=>eicar.com | N/A | WIN-68GURACIKUD | win-68guracikud | Administrator | Antimalware | 1 | 13 June 2018, 17:38:18 | Contoso systems pvt. ltd. |
| 06/18/2018 12:29:35 PM | Unconfirmed 73987.crdownload=>eicar.com | C:\Users\contoso\Downloads\Unconfirmed 73987.crdownload=>eicar.com | 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f | CONTOSO-PC | contoso-pc | contoso | Antimalware | 1 | 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\e799cc83-a245-410c-8153-55f9257dff64.tmp=>eicar.com | 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f | CONTOSO-PC | contoso-pc | contoso | Antimalware | 1 | 14 June 2018, 15:13:07 | Contoso systems pvt. ltd. |
| 06/18/2018 12:29:35 PM | calc.exe | C:\Windows\System32\calc.exe | N/A | CONTOSO-PC | contoso-pc | contoso | Content Control | 3 | 14 June 2018, 15:29:50 | Contoso systems pvt. ltd. |

Figure 12

**Sample logs:**

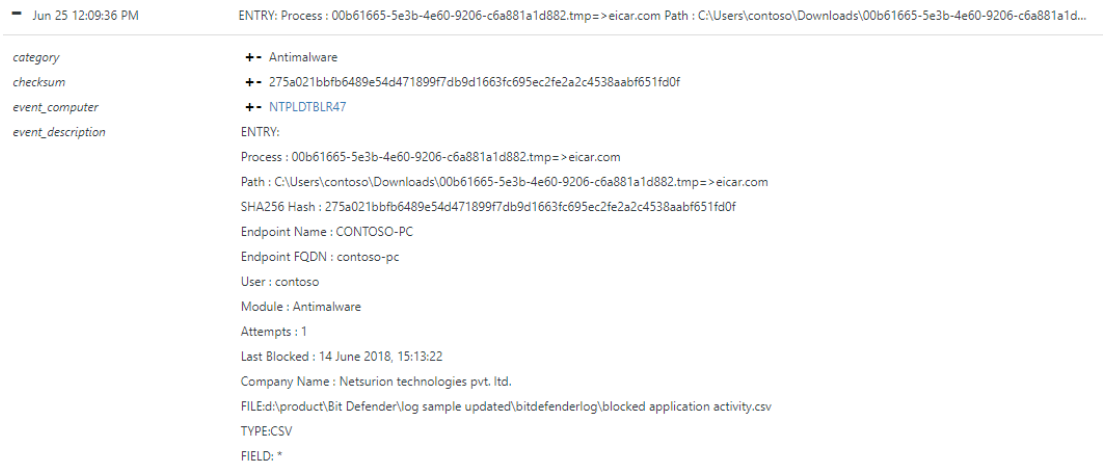


Figure 13

- **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. ltd. |
| 06/14/2018 03:30:58 PM | CONTOSO-PC | contoso-pc | https://beacons.gvt2.com/domainreliability/upload | Scheduler | Time constraint | contoso | 14 | 14 June 2018, 15:00:40 | Contoso systems pvt. ltd. |
| 06/14/2018 03:30:58 PM | CONTOSO-PC | contoso-pc | https://www.google.com/chrome/thank-you.html | Control center | malware | williams | 1 | 14 June 2018, 14:57:15 | Contoso systems pvt. ltd. |
| 06/14/2018 03:30:58 PM | CONTOSO-PC | contoso-pc | https://www.google.co.in/domainreliability/upload | Scheduler | Time constraint | contoso | 3 | 14 June 2018, 14:58:39 | Contoso systems pvt. ltd. |
| 06/14/2018 03:30:58 PM | CONTOSO-PC | contoso-pc | https://beacons5.gvt2.com/domainreliability/upload | Scheduler | Time constraint | contoso | 14 | 14 June 2018, 15:00:46 | Contoso systems pvt. ltd. |
| 06/14/2018 03:30:58 PM | CONTOSO-PC | contoso-pc | https://beacons5.gvt3.com/domainreliability/upload | Scheduler | Time constraint | contoso | 14 | 14 June 2018, 15:00:59 | Contoso systems pvt. ltd. |
| 06/14/2018 03:30:58 PM | CONTOSO-PC | contoso-pc | https://beacons4.gvt2.com/domainreliability/upload | Scheduler | Time constraint | contoso | 14 | 14 June 2018, 15:00:45 | Contoso systems pvt. ltd. |

Figure 14

**Sample logs:**

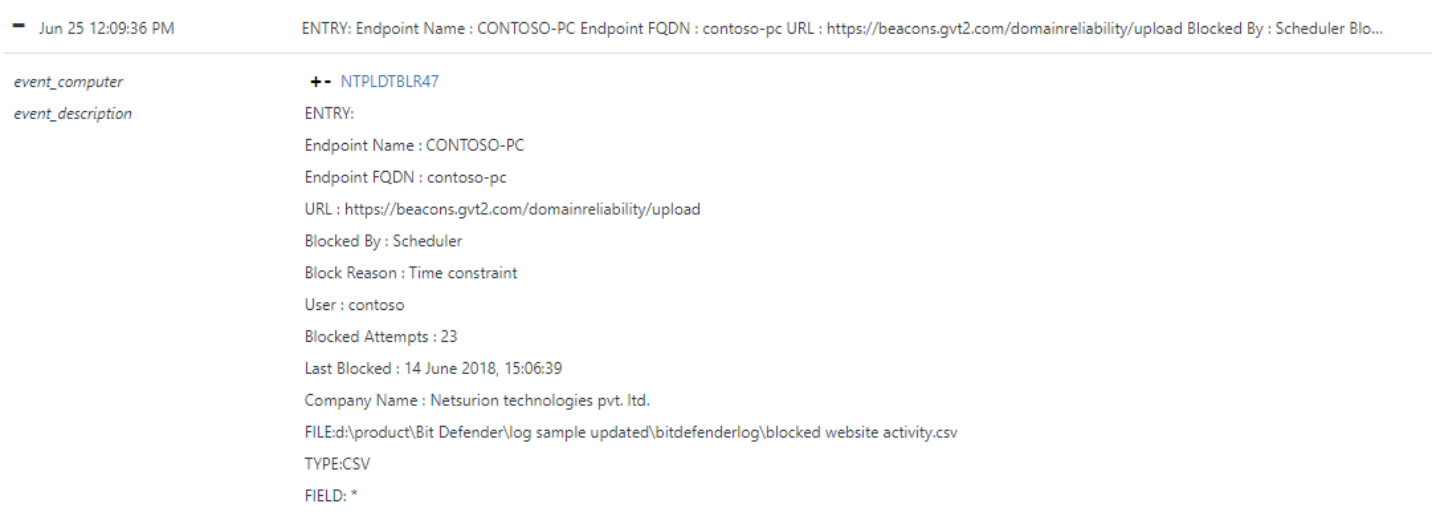


Figure 15

- **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 |

Figure 16

**Sample logs:**

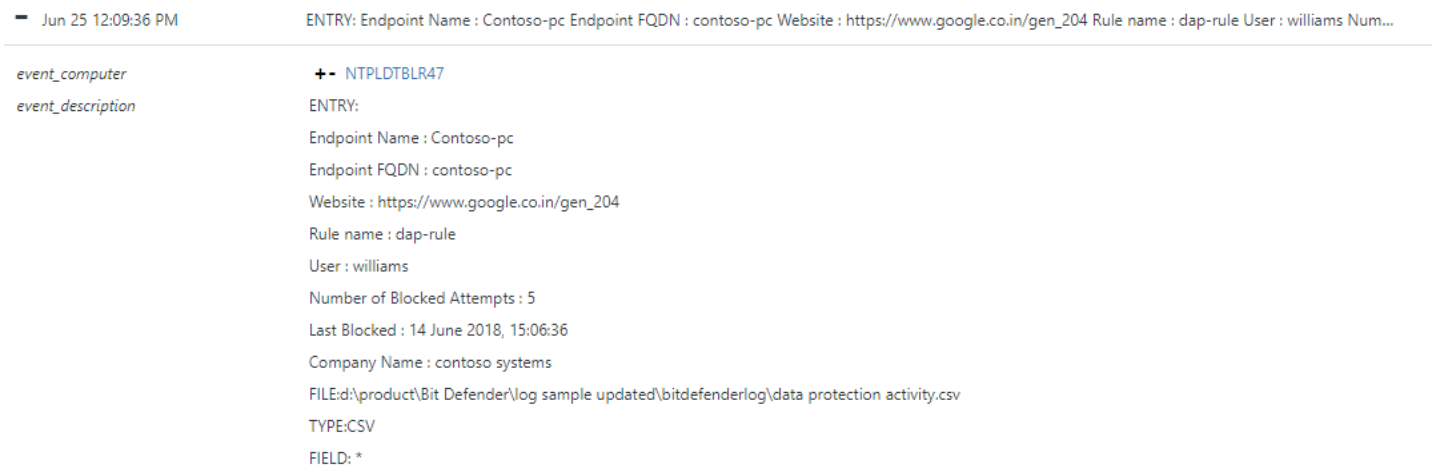


Figure 17

- **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.

| LogTime | Computer | Endpoint Name | Endpoint FQDN | Email | Rule name | User Name | Number of blocked 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:**

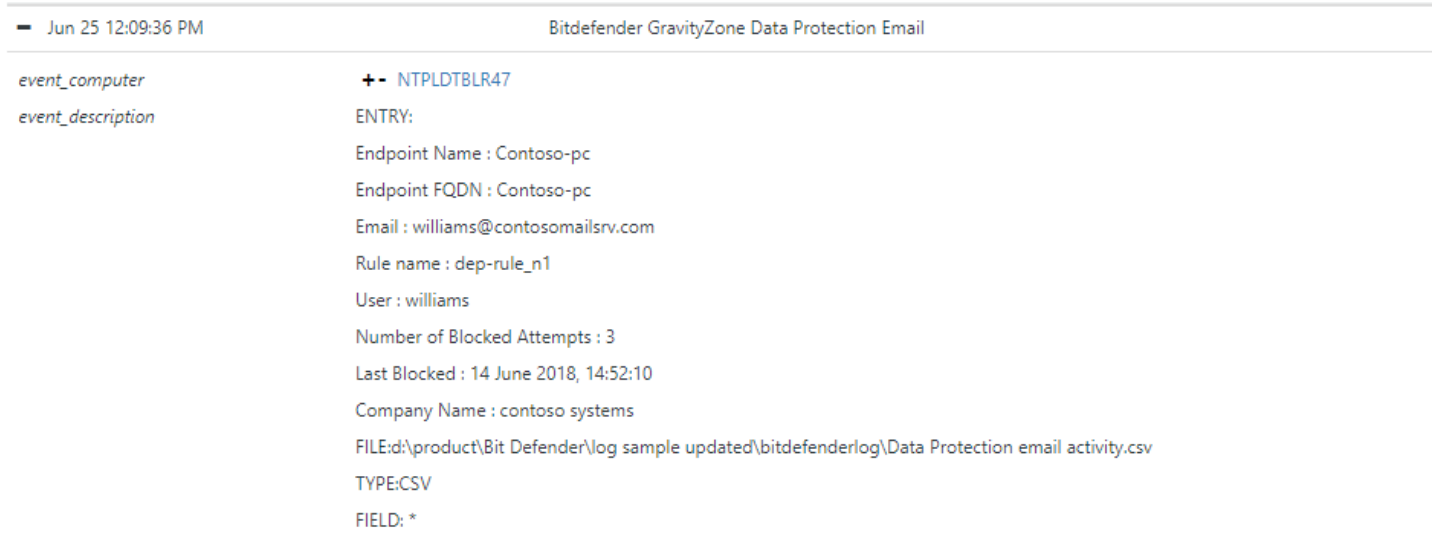


Figure 19

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

| LogTime | Computer | Date | Endpoint Name | Endpoint FQDN | Username | Status | Device Name | Device Class | Device ID | Product ID | Vendor ID | Company Name |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 06/14/2018 04:44:55 PM | NTPLDTBLR47-DLA | 14 June 2018, 14:52:10 | CONTOSO-PC | contoso-pc | contoso | Allowed | VBOX CD-ROM | External Storage | IDE\CDROMVBOX_CD-ROM_____1.0_____ | 454545 | 0 | contoso systems pvt. ltd. |
| 06/14/2018 04:44:55 PM | NTPLDTBLR47-DLA | 14 June 2018, 14:52:10 | CONTOSO-PC | contoso-pc | contoso | Blocked | CD-ROM Drive | CDROM Drive | IDE\CDROMVBOX_CD-ROM_____1.0_____\5&2117B2E5&0&1.0.0 | 0 | 0 | contoso systems pvt. ltd. |
| 06/14/2018 04:44:55 PM | NTPLDTBLR47-DLA | 14 June 2018, 14:52:10 | CONTOSO-PC | contoso-pc | contoso | Blocked | CD-ROM Drive | CDROM Drive | IDE\CDROMVBOX_CD-ROM_____1.0_____\5&2117B2E5&0&1.0.0 | 4425452 | 0 | contoso systems pvt. ltd. |

Figure 20

**Sample logs:**

| Jun 25 12:09:36 PM | Bitdefender GravityZone Device Control Activity |
|---|---|
| *addl_info1* | + - Product ID |
| *addl_info2* | + - Vendor ID |
| *category* | + - Device Class |
| *device_id* | + - Device ID |
| *device_name* | + - Device Name |
| *event_computer* | + - NTPLDTBLR47 |
| *event_description* | ENTRY:<br>Endpoint Name : Endpoint Name<br>Endpoint FQDN : Endpoint FQDN<br>Username : Username<br>Status : Status<br>Device Name : Device Name<br>Device Class : Device Class<br>Device ID : Device ID<br>Product ID : Product ID<br>Vendor ID : Vendor ID<br>Date : Date<br>Company Name : Company Name<br>FILE:d:\product\Bit Defender\log sample updated\bitdefenderlog\device control activty.csv<br>TYPE:CSV<br>FIELD: * |

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 Ip | 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 |

Figure 22

**Sample logs:**


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.

| LogTime | Endpoint Name | Endpoint FQDN | File Path | Port | Protocol | User Name | blocked attempts | Last Blocked | Company Name |
|---|---|---|---|---|---|---|---|---|---|
| 06/15/2018 02:59:46 PM | CONTOSO-PC | contoso-pc | C:\Users\contoso\Downloads\2fd92a83-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\2cdfasd.tmp | 22 | Telnet | 22 | 5 | 14 June 2018, 15:13:28 | contoso systems |

Figure 24

**Sample logs:**

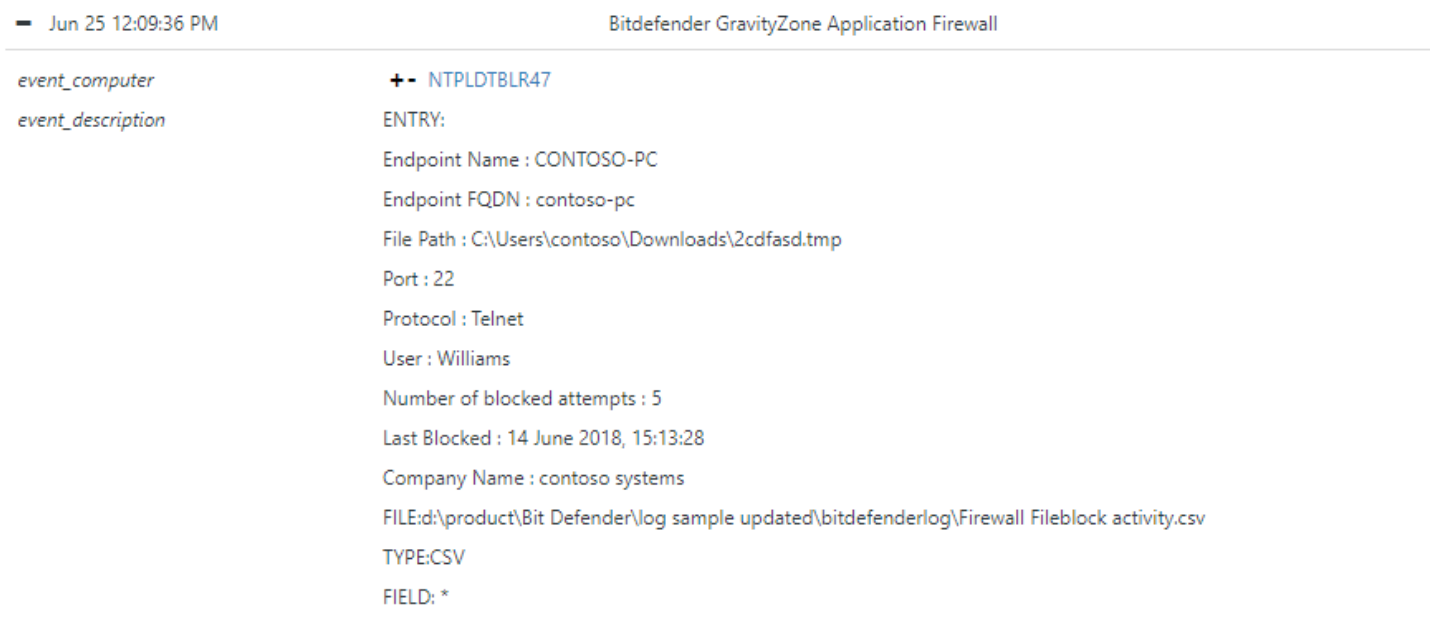


Figure 25

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

| LogTime | Computer | Endpoint 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\Downloads\2fd92a83-f7d3-4e40-8b55-95445257c59d.tmp | 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f | Still Infected | 1 | 14 June 2018, 15:13:28 | Contoso systemspvt. ltd. |
| 06/15/2018 12:28:50 PM | NTPLDTBLR47 | CONTOSO-PC | contoso-pc | contoso | EICAR-Test-File (not a virus) | C:\Users\contoso\Downloads\Unconfirmed 73987.crdownload=>eicar.com | 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f | Still Infected | 1 | 14 June 2018, 15:13:04 | Contoso systemspvt. ltd. |
| 06/15/2018 12:28:50 PM | NTPLDTBLR47 | CONTOSO-PC | contoso-pc | contoso | EICAR-Test-File (not a virus) | C:\Users\contoso\Downloads\dc2325d1-0b95-4e4c-8751-4d6663a322b4.tmp | N/A | Still Infected | 1 | 14 June 2018, 15:13:19 | Contoso systemspvt. ltd. |
| 06/15/2018 12:28:50 PM | NTPLDTBLR47 | CONTOSO-PC | contoso-pc | contoso | EICAR-Test-File (not a virus) | C:\Users\contoso\Downloads\00b61665-5e3b-4e60-9206-c6a881a1d882.tmp=>eicar.com | 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f | Resolved | 1 | 14 June 2018, 15:13:22 | Contoso systemspvt. ltd. |

Figure 26

**Sample logs:**

Jun 25 12:09:37 PM Bitdefender GravityZone Malware Activity

| | |
|---|---|
| *checksum* | 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f |
| *event_computer* | NTPLDTBLR47 |
| *event_description* | ENTRY:<br>Malware name : EICAR-Test-File (not a virus)<br>File Path : C:\Users\contoso\Downloads\e7d50fa6-b4bf-4a77-9293-31f854d384c3.tmp<br>SHA256 Hash : 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f<br>Endpoint Name : CONTOSO-PC<br>Endpoint FQDN : contoso-pc<br>User : contoso<br>Status : Resolved<br>Last Detection : 14 June 2018, 15:13:28<br>Count : 1<br>Company Name : Netsurion technologies pvt. ltd.<br>FILE:d:\product\Bit Defender\log sample updated\bitdefenderlog\malware activity.csv<br>TYPE:CSV<br>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\2fd92a83-f7d3-4e40-8b55-95445257c59d.tmp | 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f | 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\Unconfirmed 73987.crdownload=>eicar.com | 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f | 14 June 2018, 15:13:04 |
| 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\dc2325d1-0b95-4e4c-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\e799cc83-a245-410c-8153-55f9257dff64.tmp=>eicar.com | 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f | 14 June 2018, 15:13:07 |
| 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\e750fa6-b4bf-4a77-9293-31f854d384c3.tmp | 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f | 14 June 2018, 15:13:28 |

Figure 28

**Sample logs** :

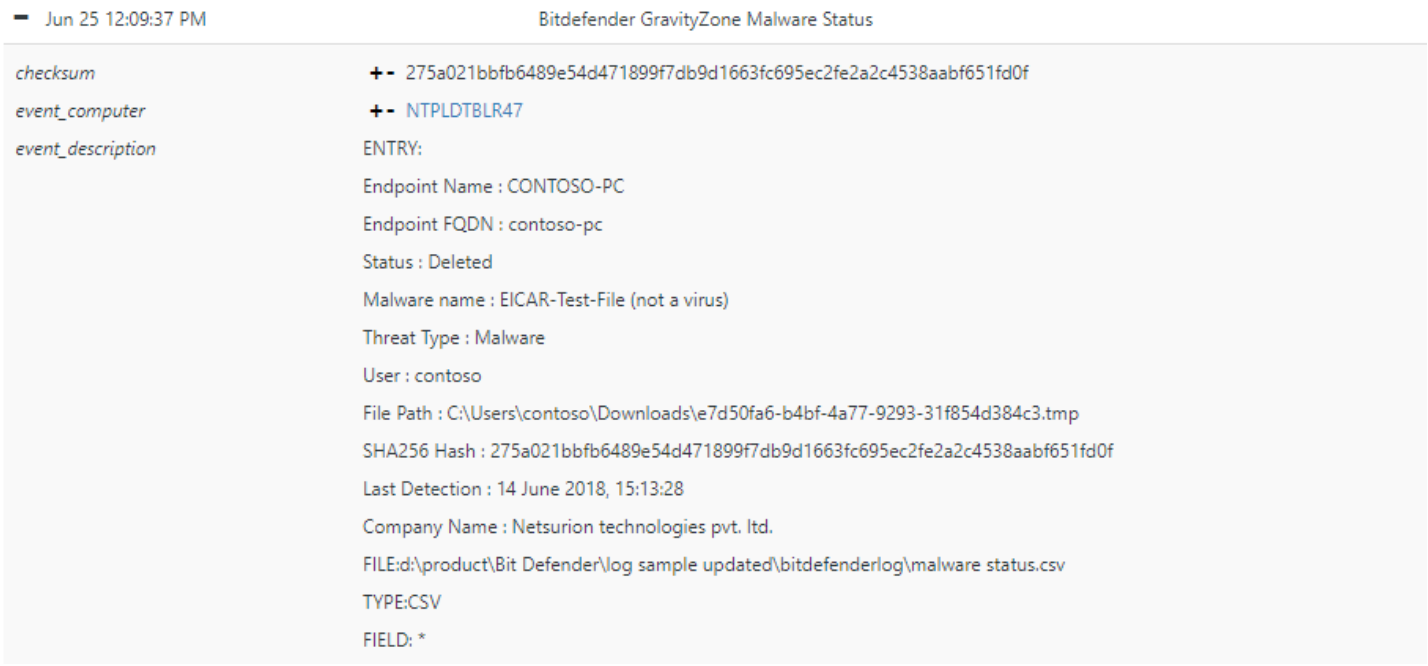


Figure 29

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

| LogTime | Computer | Endpoint Name | Endpoint FQDN | Scan Name | Scan Type | Recurrence | Successful scans | Failed scans | Last successful scan | Company Name |
|---|---|---|---|---|---|---|---|---|---|---|
| 06/15/2018 11:52:28 AM | NTPLDTBLR47 | CONTOSO-PC | contoso-pc | Daily scan | Quick Scan | Run every 1 day | 1 | 0 | 14 June 2018, 16:15:48 | Contoso systemspvt. ltd. |
| 06/15/2018 11:52:28 AM | NTPLDTBLR47 | CONTOSO-PC | contoso-pc | Week end scan | Quick Scan | Run every 1 week | 1 | 0 | 14 June 2018, 16:15:48 | Contoso systemspvt. ltd. |
| 06/15/2018 11:52:28 AM | NTPLDTBLR47 | CONTOSO-PC | contoso-pc | Daily scan | Quick Scan | Run every 1 day | 1 | 0 | 14 June 2018, 16:15:48 | Contoso systemspvt. ltd. |
| 06/15/2018 11:52:28 AM | NTPLDTBLR47 | CONTOSO-PC | contoso-pc | Daily scan | Quick Scan | Run every 1 day | 1 | 0 | 14 June 2018, 16:15:48 | Contoso systemspvt. ltd. |

Figure 30

**Sample logs:**

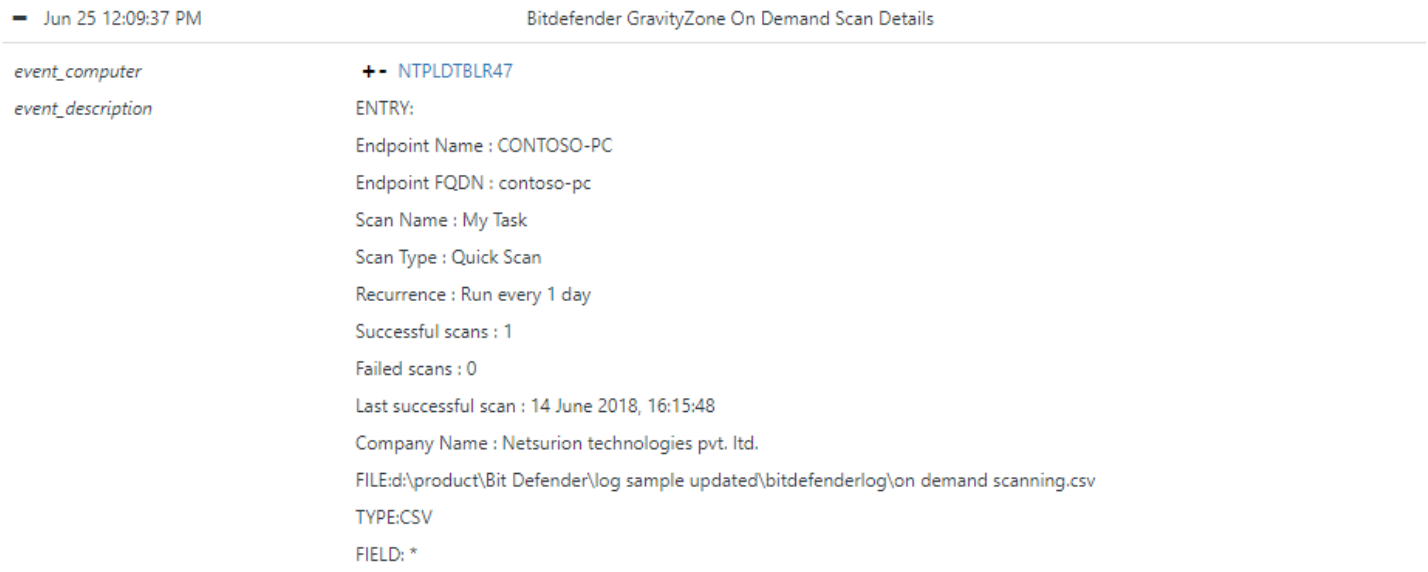


Figure 31

- **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\2fd92a83-f7d3-4e40-8b55-95445257c59d.tmp, SHA256 Hash: 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f, Malware Name: EICAR-Test- | 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f, Malware Name: EICAR-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 | 1 | Antimalware | Malware Detection | File Path: C:\Users\contoso\Downloads\Unconfirmed 73987.crdownload=>eicar.com, SHA256 Hash: 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f, Malware Name: EICAR-Test- | 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f, Malware Name: EICAR-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 | 1 | Antimalware | Malware Detection | File Path: C:\Users\contoso\Downloads\dc2325d1-0b95-4e4c-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 |

Figure 32

**Sample logs:**

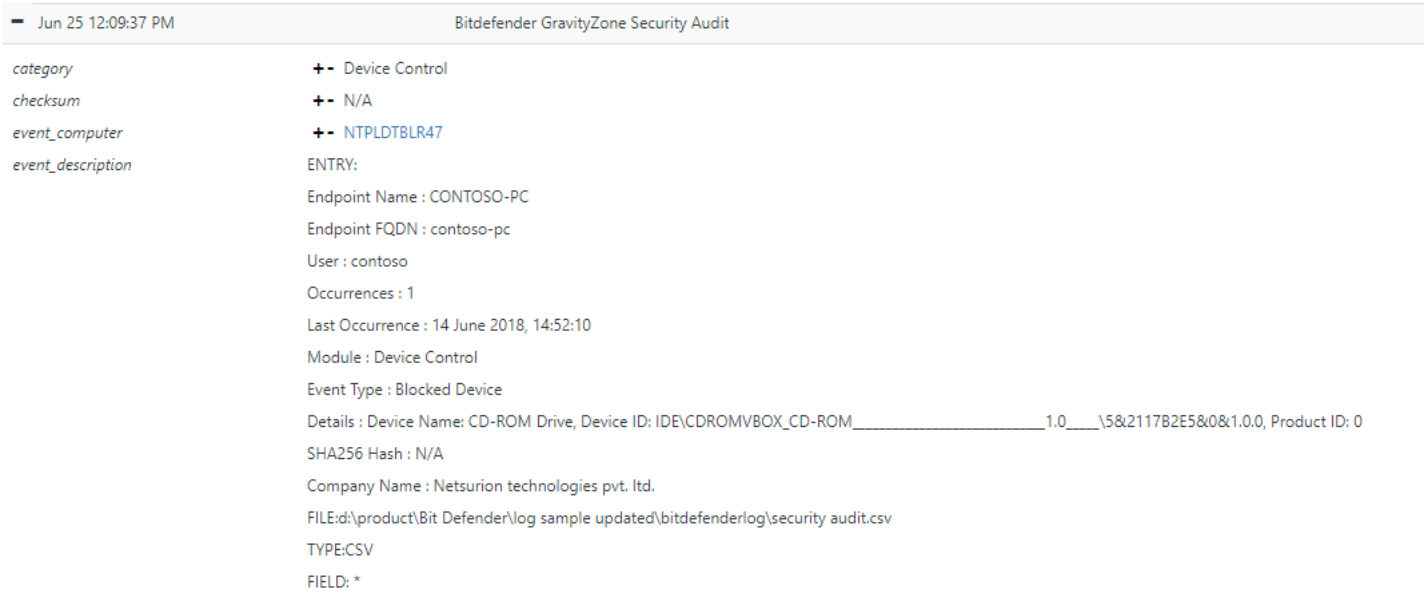


Figure 33

# 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**.

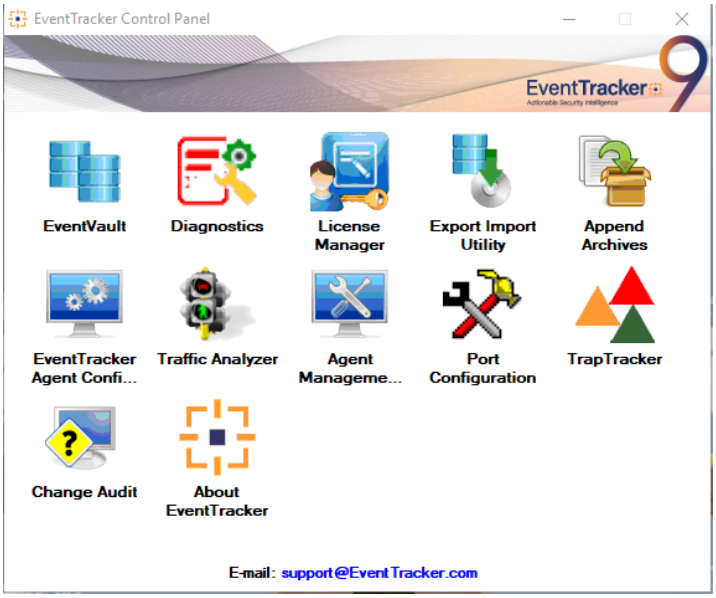


Figure 34

3. Click the **Import** tab.

## Category

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

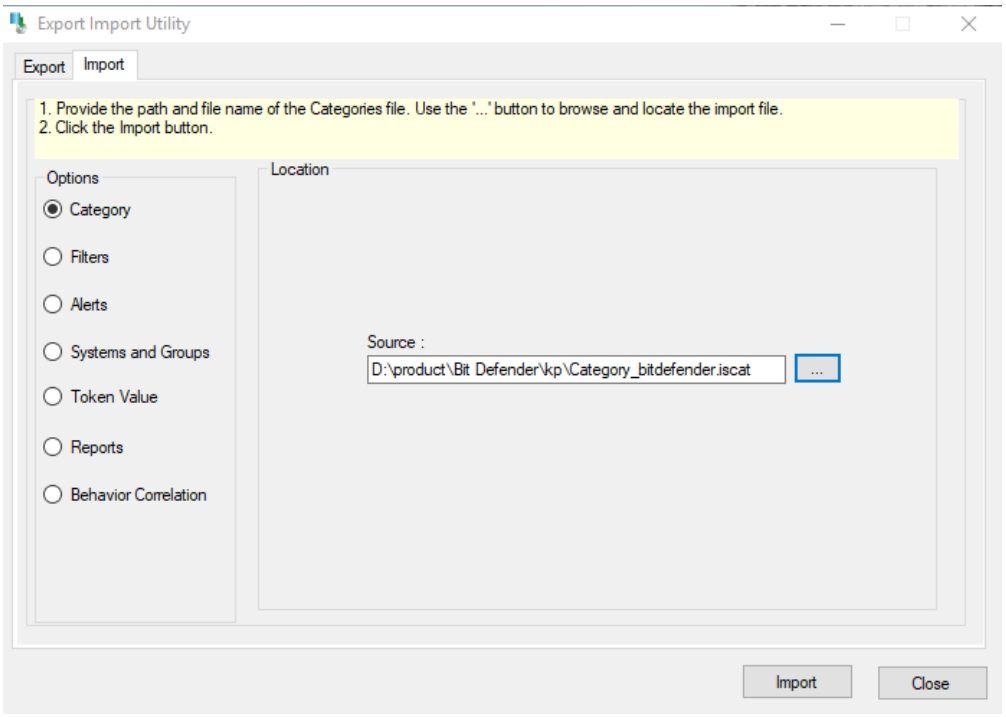


Figure 35

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.

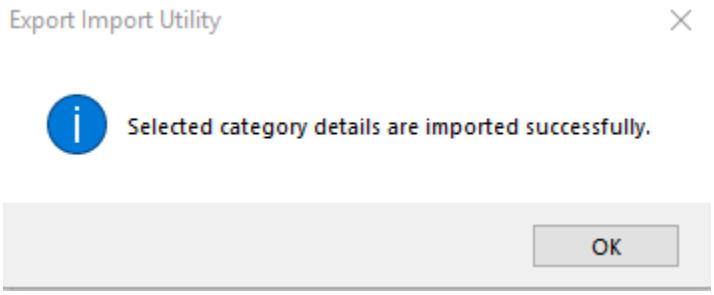


Figure 36

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**.

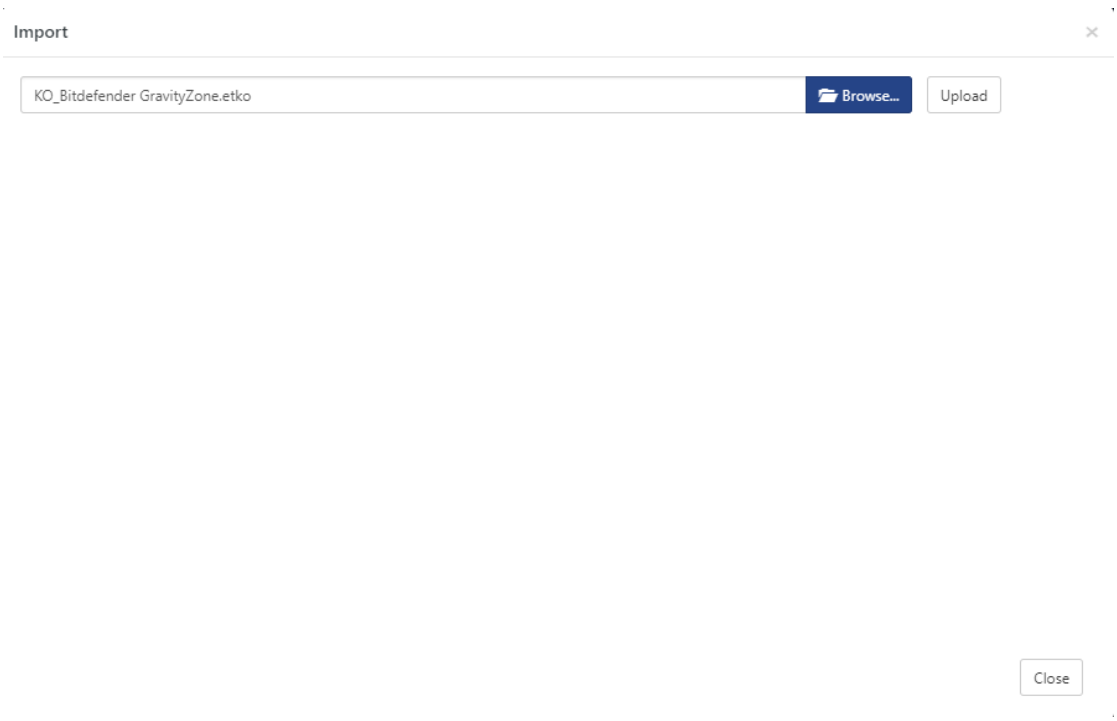


Figure 37

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

| Object name | Applies to | Group name |
|---|---|---|
| Bitdefender GravityZone Antiphishing Activity | Bitdefender GravityZone | Bitdefender GravityZone |
| Bitdefender GravityZone Application Firewall | Bitdefender GravityZone | Bitdefender GravityZone |
| Bitdefender GravityZone Blocked Applications | Bitdefender GravityZone | Bitdefender GravityZone |
| Bitdefender GravityZone Blocked Website Details | Bitdefender GravityZone | Bitdefender GravityZone |
| Bitdefender GravityZone Data Protection Email | Bitdefender GravityZone | Bitdefender GravityZone |
| Bitdefender GravityZone Data Protection Web | Bitdefender GravityZone | Bitdefender GravityZone |
| Bitdefender GravityZone Device Control Activity | Bitdefender GravityZone | Bitdefender GravityZone |
| Bitdefender GravityZone Firewall Activity | Bitdefender GravityZone | Bitdefender GravityZone |
| Bitdefender GravityZone Malware Activity | Bitdefender GravityZone | Bitdefender GravityZone |
| Bitdefender GravityZone Malware Status | Bitdefender GravityZone | Bitdefender GravityZone |
| 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.

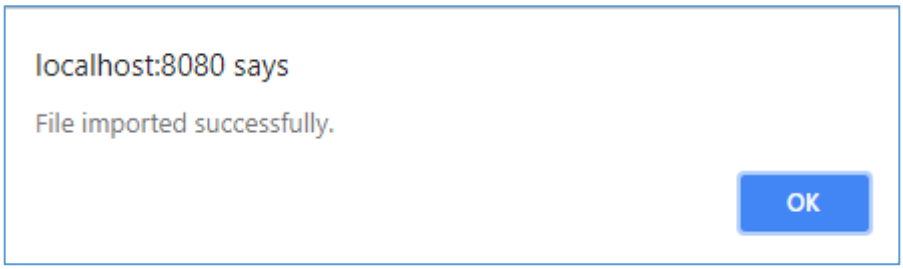


Figure 39

# Flex Reports

On EventTracker Control Panel,

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

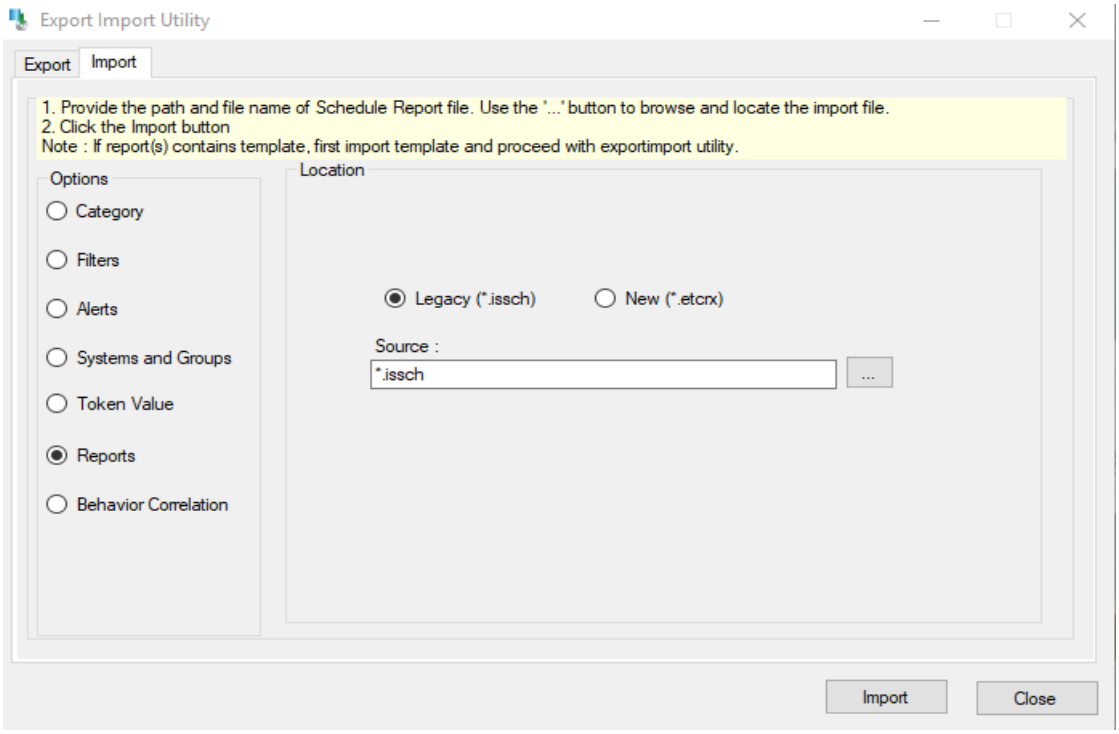


Figure 40

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

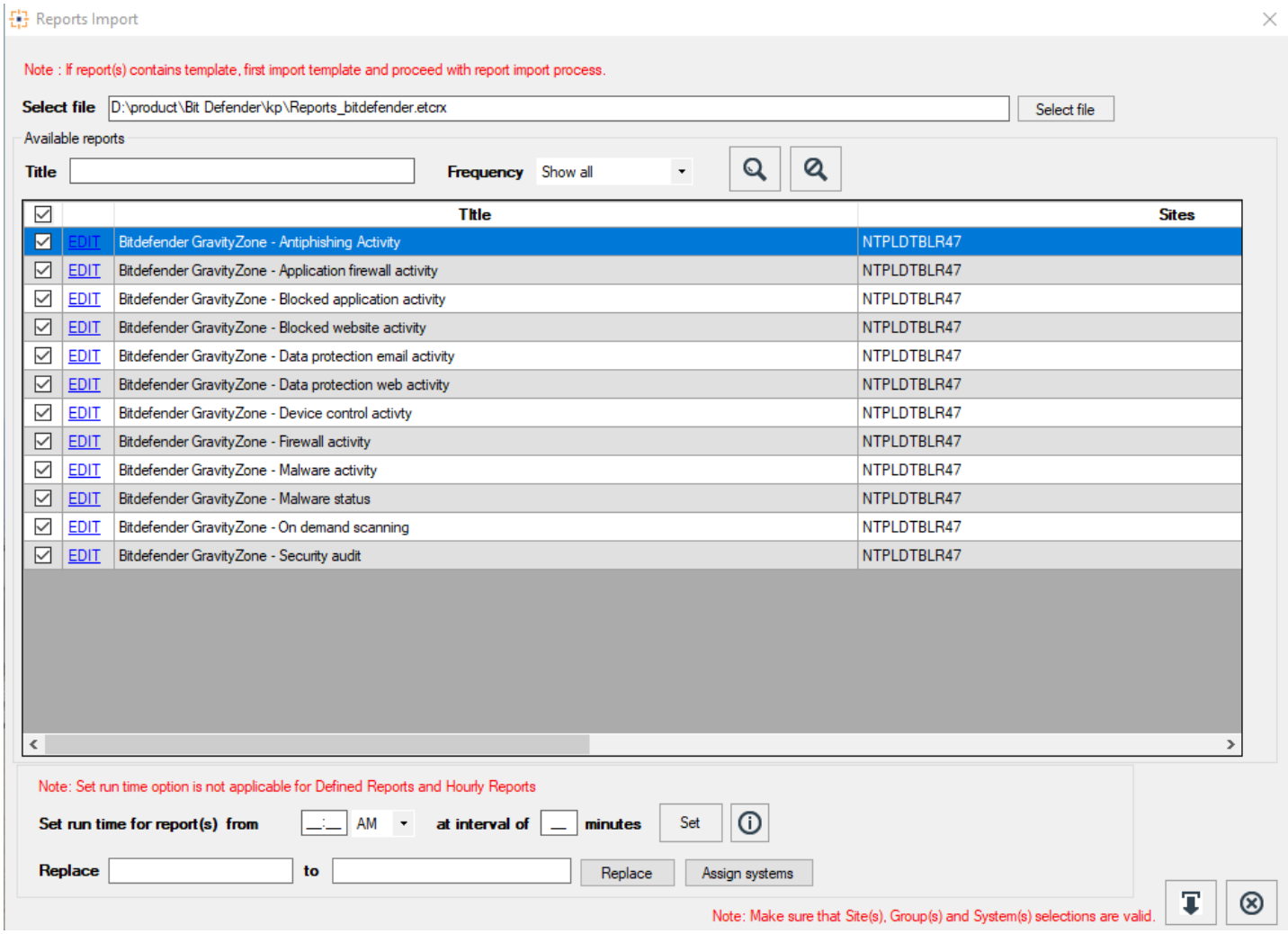


Figure 41

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

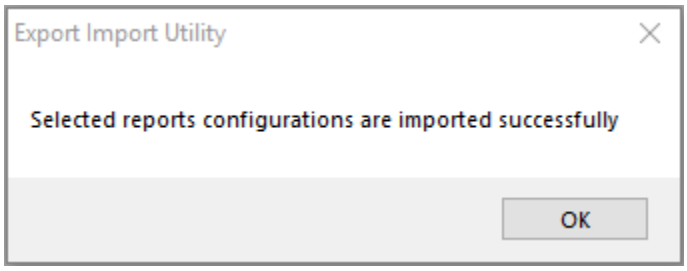


Figure 42

# Dashlets

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

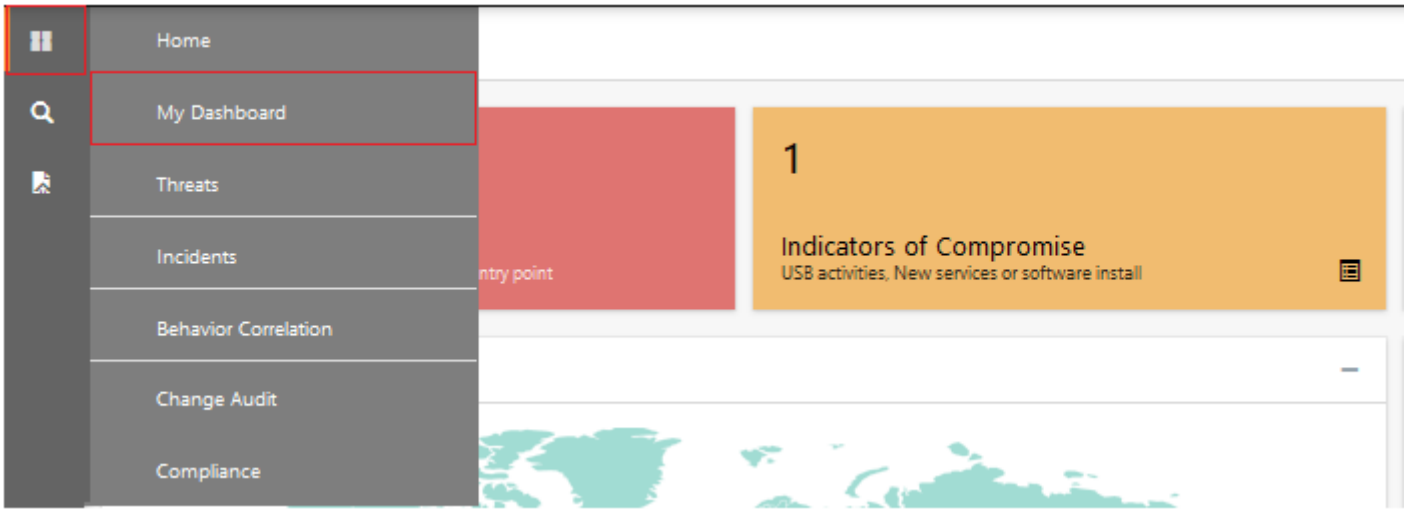


Figure 43

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

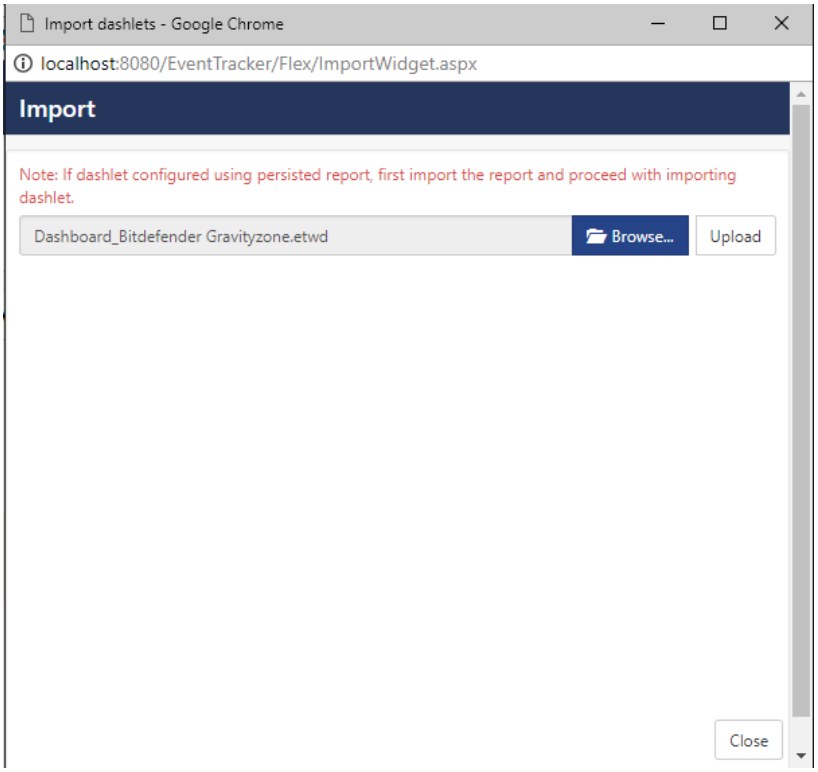


Figure 44

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

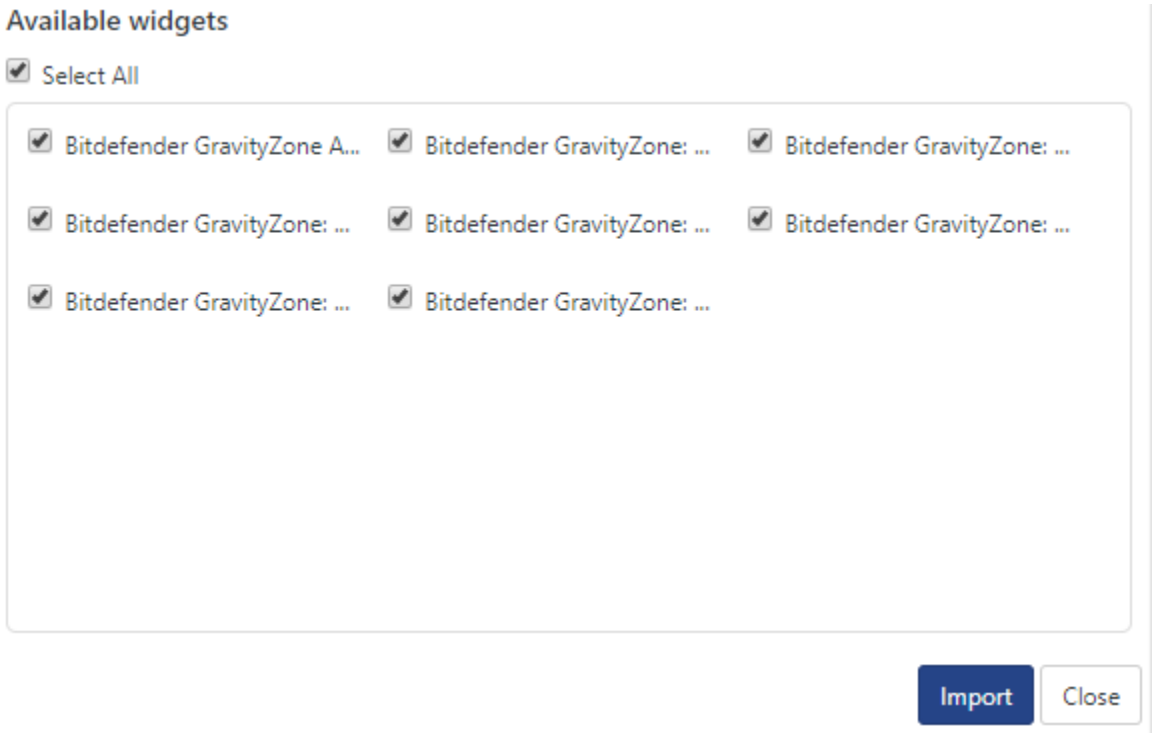


Figure 45

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

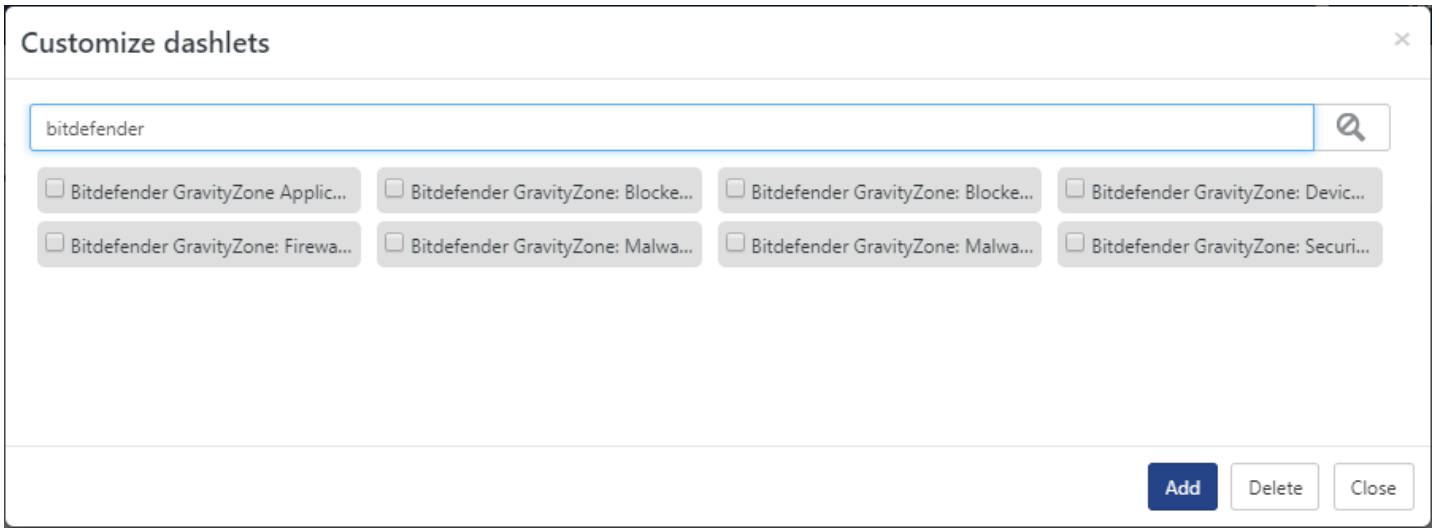


Figure 46

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.

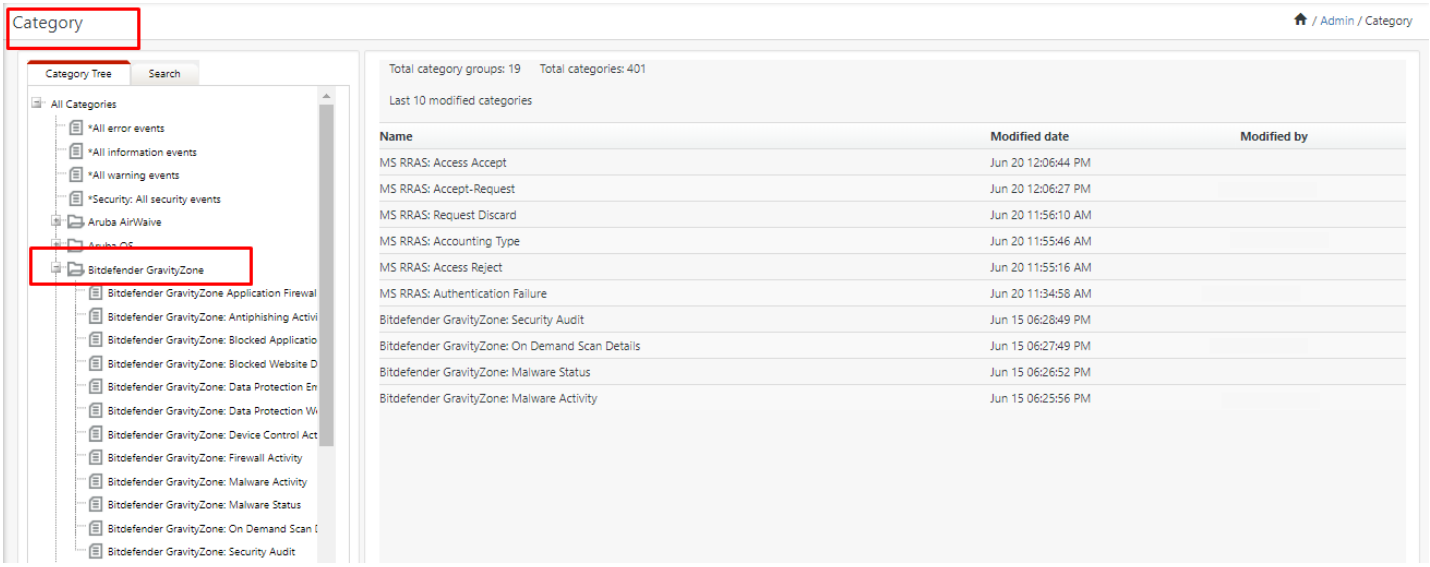


Figure 47

## 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.

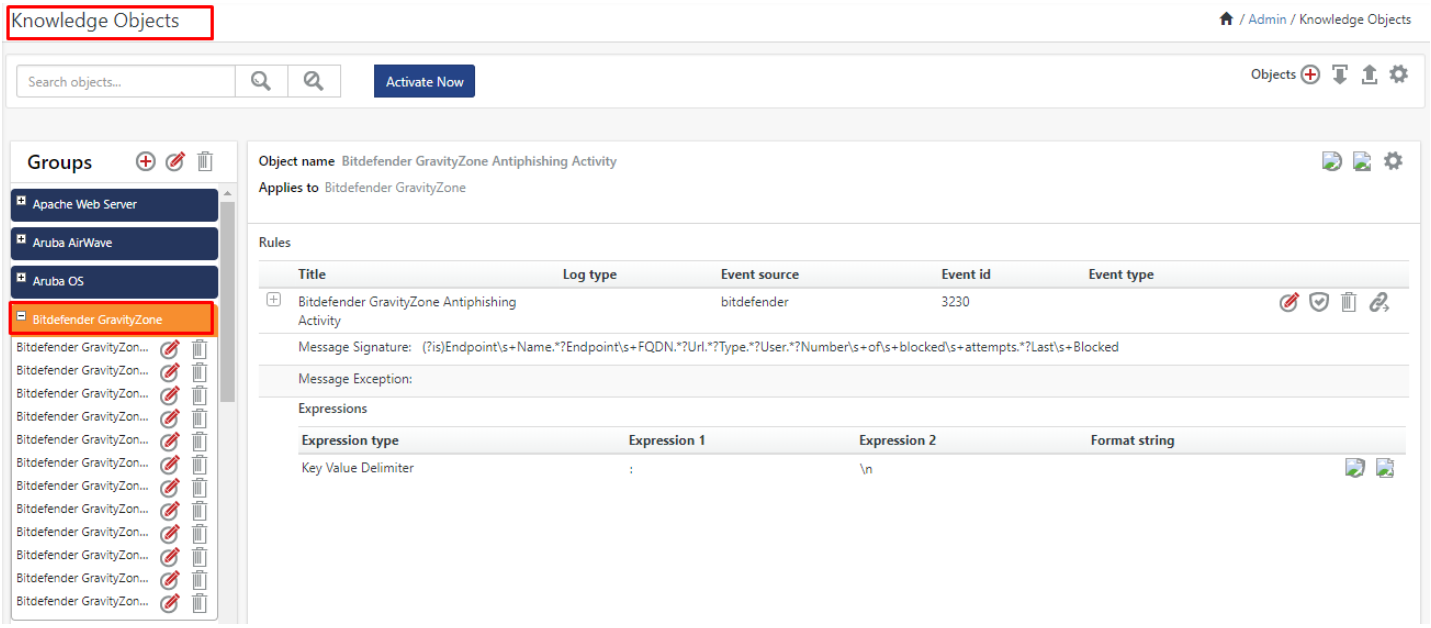


Figure 48

# Flex Reports

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

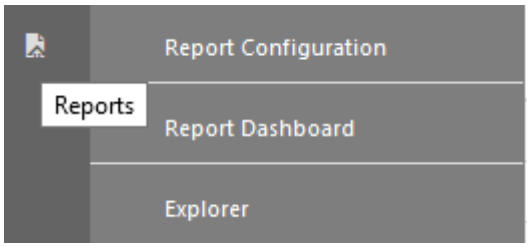


Figure 49

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

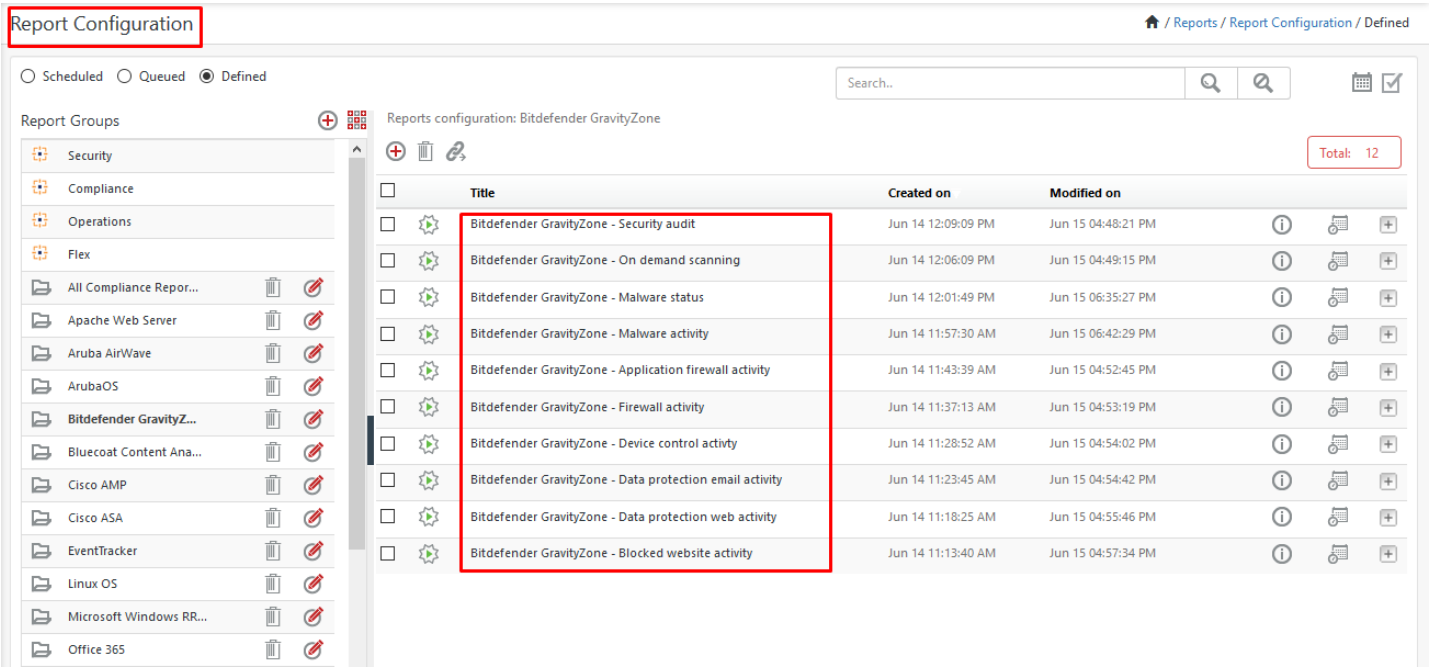


Figure 50

# Sample Flex Dashboards

**Title:** Bitdefender GravityZone Application Firewall

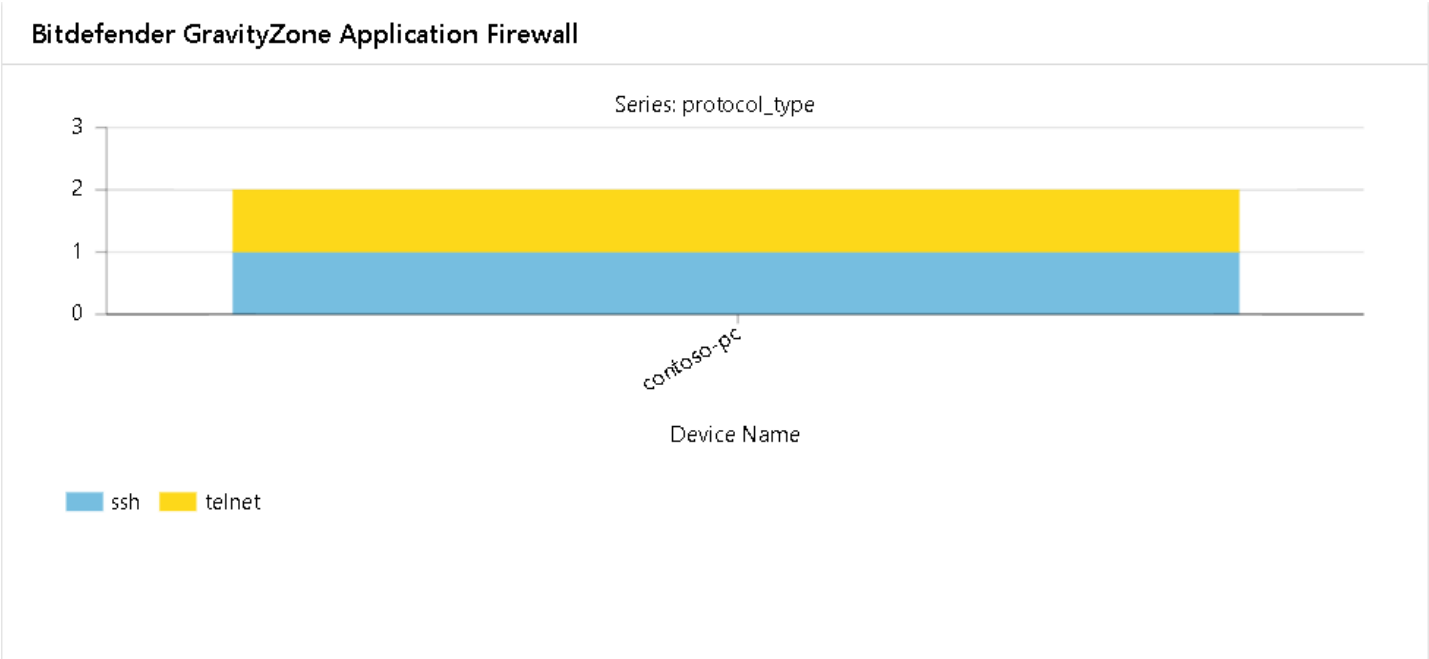


Figure 51

**Title:** Bitdefender GravityZone Blocked Application

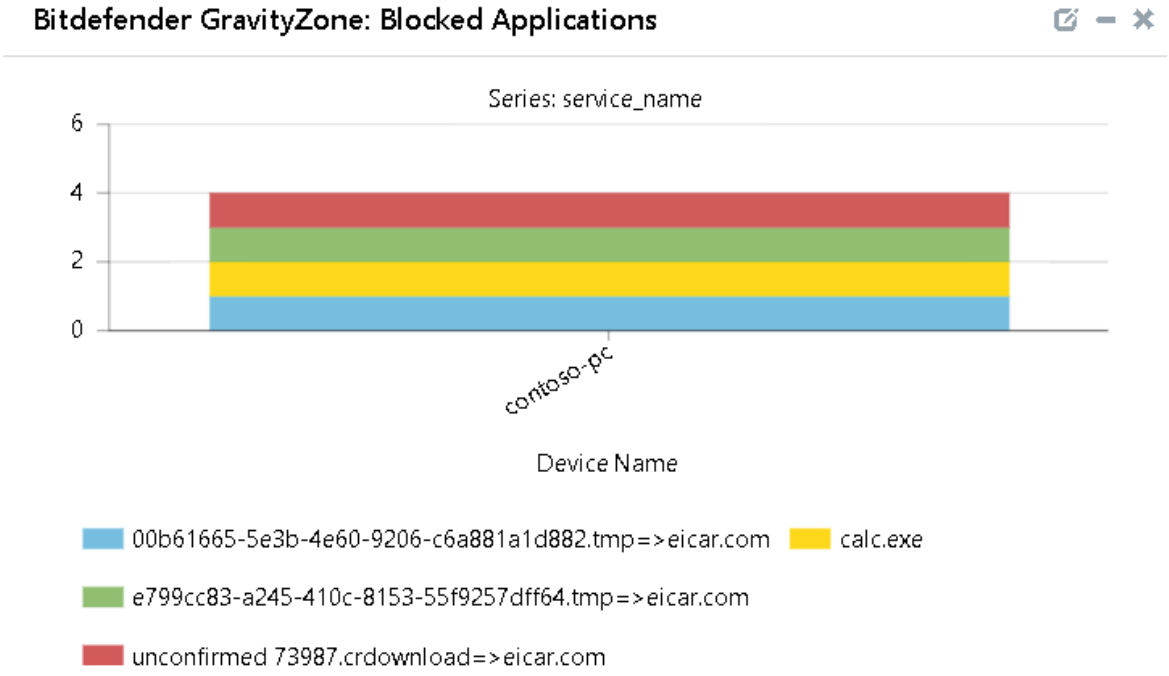


Figure 52

**Title:** Bitdefender GravityZone Blocked Websites

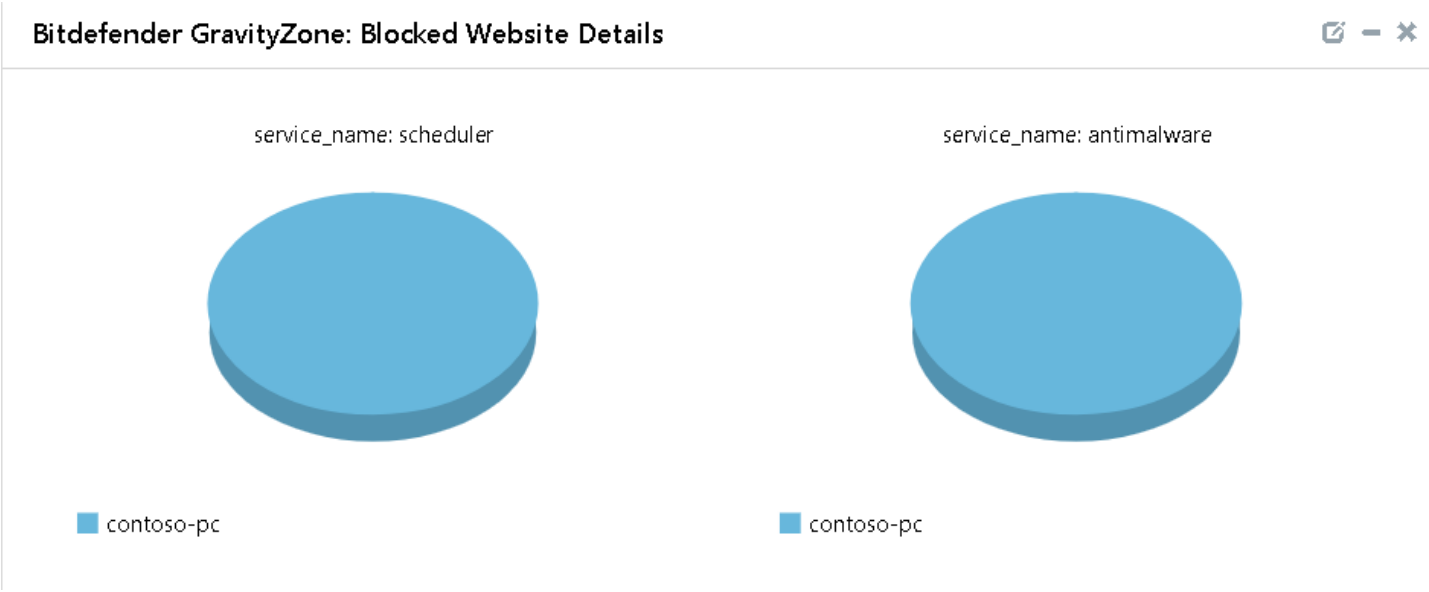


Figure 53

**Title:** Bitdefender GravityZone Firewall Activity

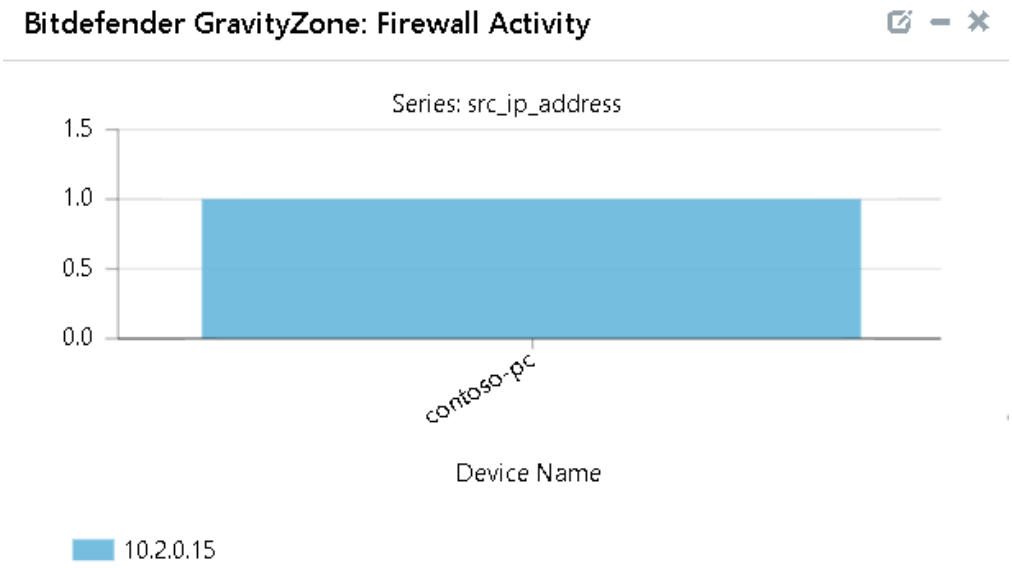


Figure 54

**Title:** Bitdefender GravityZone Malware Activity

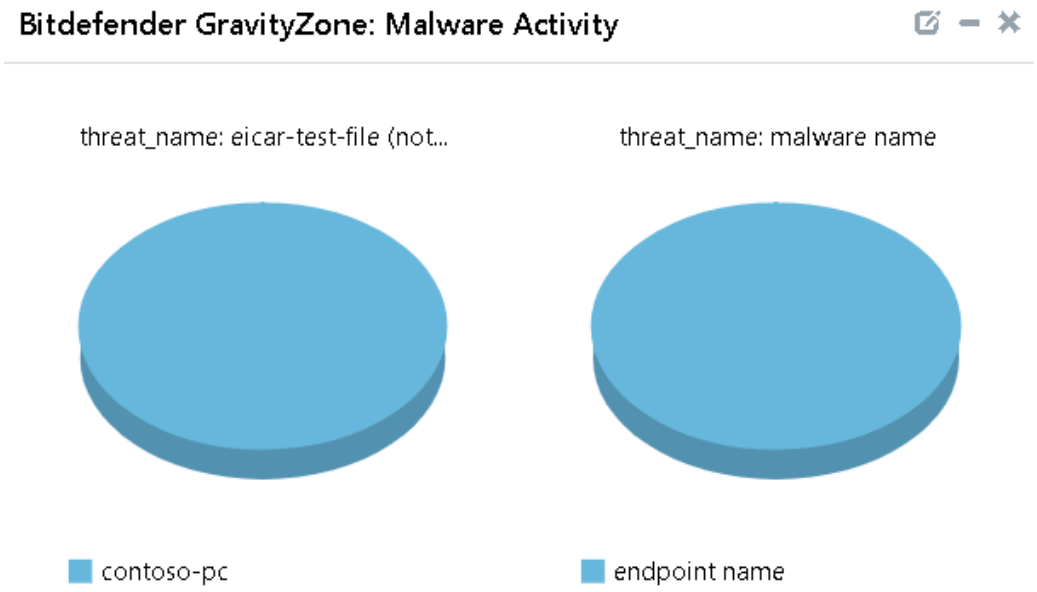


Figure 55

**Title:** Bitdefender GravityZone Malware Status

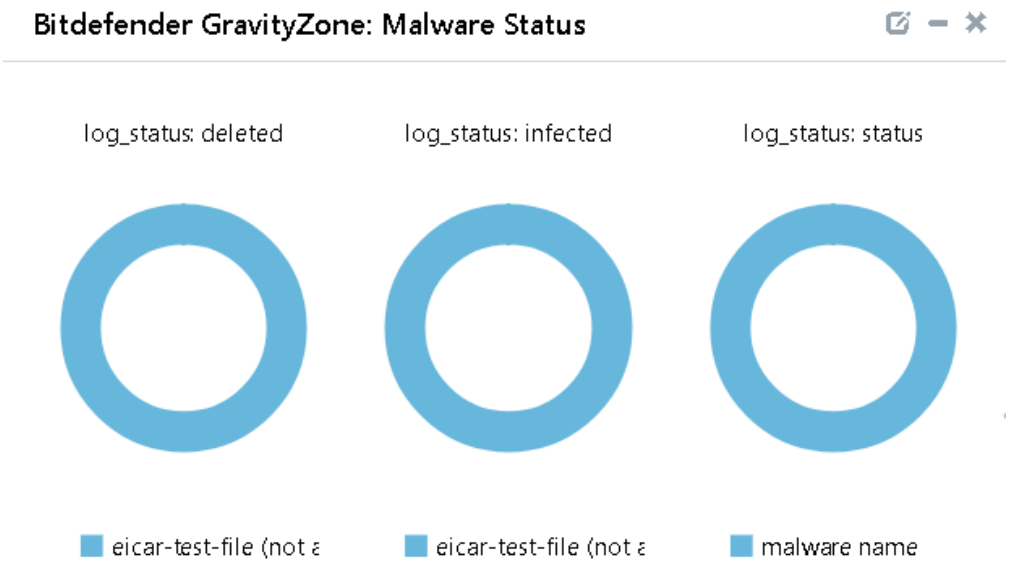


Figure 56

**Title:** Bitdefender GravityZone Device Control Activity

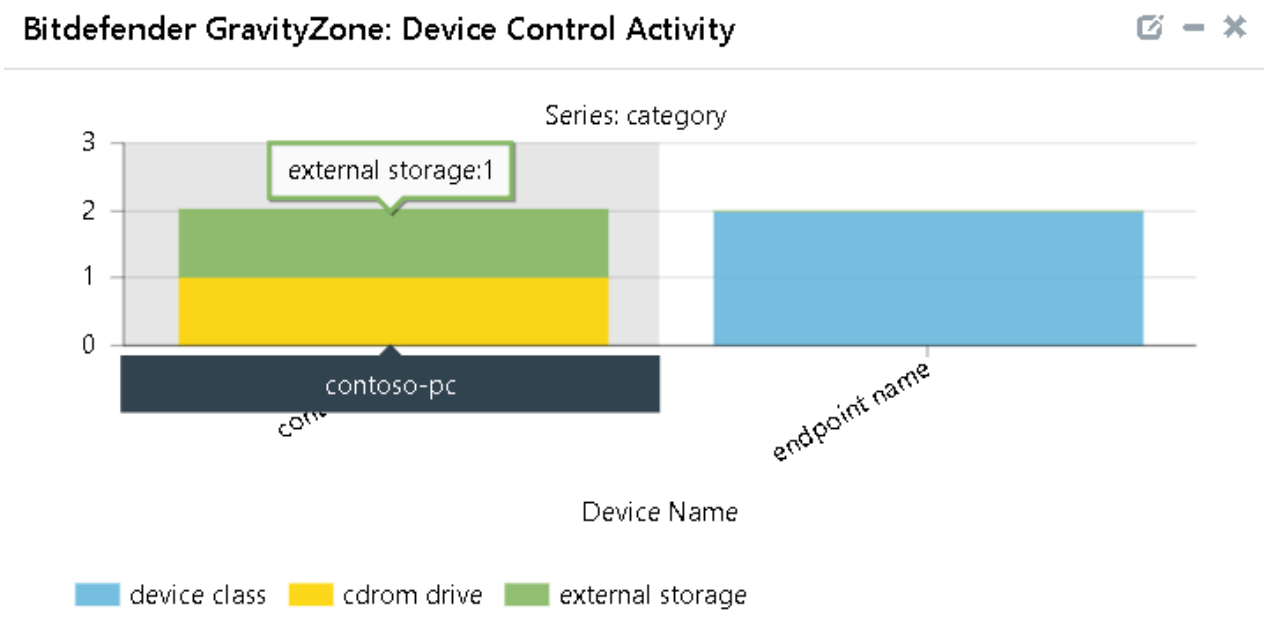


Figure 57

**Title:** Bitdefender GravityZone Security Audit

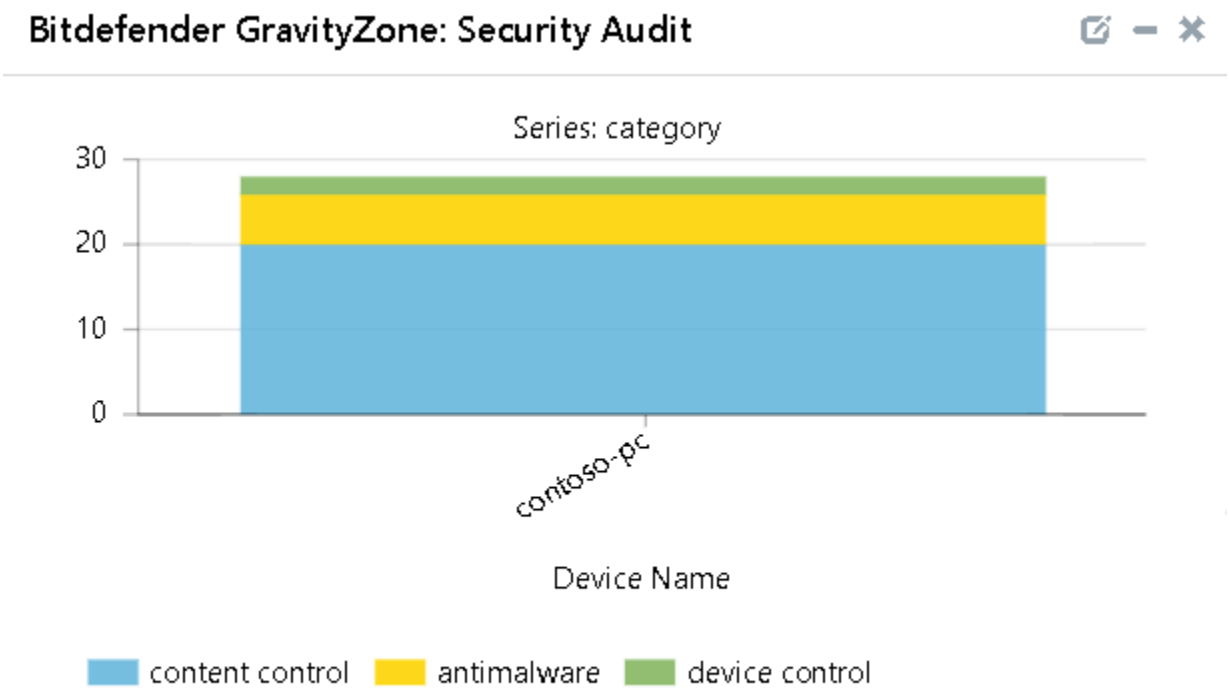


Figure 58