Cloud DDoS Protection Demo Guide for Partners

Written by Daniel Offek

Advanced Solutions, Security AMS

Version 1.0

February, 2023

TABLE OF CONTEXT

Introduction

Welcome to Radware's Cloud DDoS Demo guide. This guide is designed to help you effectively showcase the powerful capabilities of Radware's cloud DDoS solution for customers. DDoS attacks are a growing concern for businesses of all sizes and types, and Radware's solution provides a comprehensive offering to protect against these threats.

The guide gives you the tools and resources needed to successfully demonstrate Radware's cloud DDoS solution, highlight the benefits of using it, and explain how it can protect your customers' online assets and infrastructure from DDoS attacks. The guide includes a step-by-step process for preparing and conducting the demo.

Key Presentation Messages

When delivering the demonstration, it's important to clearly communicate the following messages to potential customers. These messages will help highlight the value and benefits of the solution being presented.

Message 1: Radware offers comprehensive infrastructure and application protection, including DDoS protection, GEO blocking, Active Attacker protection, firewall/intrusion prevention system (infrastructure protection), and web application firewall, bot protection, API protection, browser-side protection, and mobile app protection (application protection). The CDDoS demo highlights the infrastructure protection aspect of Radware through the CDDoS feature.

Message 2: The Always-On mode provides optimal and continuous protection, with services like GEO, EAAF, and FW/IPS that are effective with every packet.

Message 3: The OnDemand approach features monitoring through NetFlow and includes an auto-triggered diversion feature. For customers who prefer manual control, activating diversion is straightforward and simple through the portal.

Message 4: The Behavioral DOS protection engine is the most robust and can quickly recognize and block attack footprints within seconds. The unique footprint identification ensures zero false positives and minimal disruption to legitimate traffic.

Message 5: Obtaining graphical reports to share within the organization is effortless, as they display all blocked attacks.

Message 6: The Network Analytics operates in both Always-On and OnDemand modes, offering insights into enterprise traffic patterns, top users, and top applications. This provides visibility for network and security planning to both the network and security operator.

Prerequisites

The purpose of this section is to ensure that you are fully prepared and equipped with the necessary tools and knowledge to effectively demonstrate the capabilities of Radware's cloud DDoS solution to potential customers. Before proceeding with the demo, it is crucial to make sure that the following steps are taken to guarantee a smooth and successful demonstration:

1. Make sure you are able to access the Cloud DDoS Self Service Portal by Browsing to: https://console.radwarecloud.com. If you do not have access, please contact your account manager or our support team to request access.
2. Using the provided PowerPoint presentation, make sure the customer understands the topology of our scenario - including the attacks, legitimate traffic, target server, and our Always-On DNS diversion scenario.
3. Watch the provided Demo video for a comprehensive overview of the presentation approach.
4. This demo utilizes DNS diversion for ease of use; however, a BGP-based diversion is more commonly used to protect entire assets. Review all relevant documentation, such as the product data sheet and user guide, to gain a thorough understanding of Radware's Cloud DDoS solution. Familiarize yourself with the product's features and capabilities to effectively showcase them to customers.

Demo Overview & Flow

This demo provides a comprehensive overview of key sections of the portal, covering the Overview, Security Events, Notifications, Reports, and Analytics. Each section begins with an Action followed by a Description. The Action outlines the key points to be covered during the demo while the Description provides in-depth information to effectively demonstrate the capabilities of the Cloud DDoS portal.

Demo Summary

1. Overview
   a. Point out that the Cloud DDoS portal is accessed by clicking on the **Infrastructure Protection** button: Infrastructure Protection. Most of the features are quite different between Application Protection and Infrastructure Protection, and it is important to click the correct button to display Infrastructure Protection.
   b. Introduce the five panes on the screen: Left sidebar, Quick navigation bar, Traffic Graph, Security Events, and Insights.
   Note: You can ignore the Operational Events for this demo
   c. Left Sidebar:
      i. Give an overview of the left navigation menu.
      ii. Demonstrate the on/off toggle button for switching between Light and Dark modes.
   d. Quick Navigation Bar:
      i. Explain the purpose of the quick navigation bar and its items.
   e. Traffic Graph:
      i. Discuss the traffic graph, showing how it displays attacks and legit traffic.
      ii. How legit traffic is not impacted.
      iii. How to interact with the graph map to filter specific traffic.
      iv. How to change the graph time-range to a week and a month view.
   f. Security Events:
      i. Describe the security events, explaining the correlation between events and the graph.
      ii. Show how each attack has a corresponding event,
      iii. Expand one attack as an example to demonstrate how the real-time signature was used to mitigate it.
   g. Insights:
      i. Explain the value of insights.

ii. Focus on the "Top Attack Vectors" and "Top Attack Protocols" and how they relate to our traffic.

h. Asset

i. Click on the "Total Assets" button and explain the two existing asset types in the Asset Section.

ii. Explain the On-Demand vs Always-On modes Cloud DDoS support.

iii. Explain the ability to divert and undivert an asset from the cloud.

2. Security Events

a. Select the Security Events from the left sidebar. Make sure the Infrastructure Protection button is pressed, not the Application Protection button.

b. Explain how this page is different from the real-time view seen in the Overview section.

c. Show the capability to filter by category and severity.

3. Analytics

a. Select Analytics from the left side menu.

b. Explain this is an Add-On service.

c. Discuss the value of analytics.

d. Explain and how it can be used even when an asset is off cloud.

e. Explain the graph data points difference in relation to real time graph.

f. Go through each widget:

i. Graph view of Sites and Assets, explain the Asset Total & Asset Total History.

ii. Top source by country.

iii. Top services.

iv. Top source IP addresses.

v. Top conversations.

4. Notifications

a. Select Notifications from the left side menu.

b. Highlight the value of notifications.

c. Show the existing security & operational notifications and explain their configuration.

5. Reports

a. Select Reports from the left side menu.

b. Discuss the value of reports.

c. Explain existing types of reports.

d. Download an "Overview" type report to show its contents.

Detailed Guide

Overview Page

Action:

1. Point out that the Cloud DDoS portal is accessed by clicking on the **Infrastructure Protection** button. features are quite different between Application Protection and Infrastructure Protection, and it is important to click the correct button to display Infrastructure Protection.
2. Introduce the five panes on the screen: Left sidebar, Quick navigation bar, Traffic Graph, Security Events, and Insights.
   Note: You can ignore the Operational Events for this demo
3. Left Sidebar:
   a. Give an overview of the left navigation menu.
   b. Demonstrate the on/off toggle button for switching between Light and Dark modes.
4. Quick Navigation Bar:
   a. Explain the purpose of the quick navigation bar and its items.
5. Traffic Graph:
   a. Discuss the traffic graph, showing how it displays attacks and legit traffic.
   b. How legit traffic is not impacted.
   c. How to interact with the graph map to filter specific traffic.
   d. How to change the graph time-range to a week and a month view.
6. Security Events:
   a. Describe the security events, explaining the correlation between events and the graph.
   b. Show how each attack has a corresponding event,
   c. Expand one attack as an example to demonstrate how the real-time signature was used to mitigate it.
7. Insights:
   a. Explain the value of insights.
   b. Focus on the "Top Attack Vectors" and "Top Attack Protocols" and how they relate to our traffic.
8. Asset
   a. Click on the "Total Assets" button and explain the two existing asset types in the Asset Section.
   b. Explain the On-Demand vs Always-On modes Cloud DDoS support.
   c. Explain the ability to divert and undivert an asset from the cloud in this section.

Description:

We'll start our demo by providing a clear breakdown of the portal's structure, making it easy to navigate and understand. From there, we'll delve deeper into each aspect of the Overview section, giving the customer a comprehensive understanding of its features and capabilities.

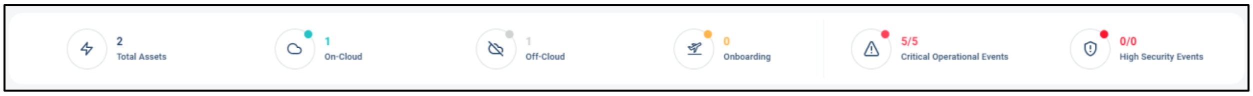
Left-Side Menu

Our left-side menu is the primary navigation tool that provides easy access to all the different features and functionalities of the portal. It is organized in a logical and intuitive way, allowing users to easily find and access the sections they need. The menu items are clearly labeled according to their purpose, making it easy for users to quickly locate the information they need.

Additionally, an on/off toggle button exists at the button of the bar for switching between Light and Dark mode.

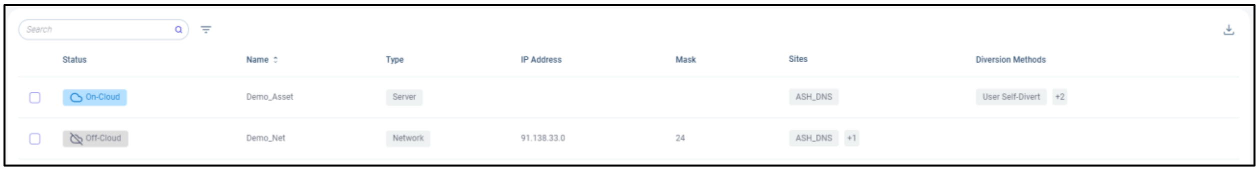
Quick Navigation Bar:

The Quick Navigation Bar allows for quick and easy access to specific sections of the portal through predefined filters, organized by their respective titles. Basically, enabling swift navigation to on\off Assets, Critical Operations and High Severity Security Events.



2	1	1	0	5/5	0/0
Total Assets	On-Cloud	Off-Cloud	Onboarding	Critical Operational Events	High Security Events

By clicking "Total Assets" you'll be taken to the Asset screen where in our demo, we have two assets: "Demo_Asset" that is on cloud (diverted), and the "Demo_Net" that is off cloud (undiverted). Each has its own type: Server and Network respectively. From the Asset screen, customers can manage their assets to manually control diversion\undiversion as needed in an On-Demand topology.



	Status	Name	Type	IP Address	Mask	Sites	Diversion Methods
□	On-Cloud	Demo_Asset	Server			ASH_DNS	User Self-Divert +2
□	Off-Cloud	Demo_Net	Network	91.138.33.0	24	ASH_DNS +1	

Traffic Graph:

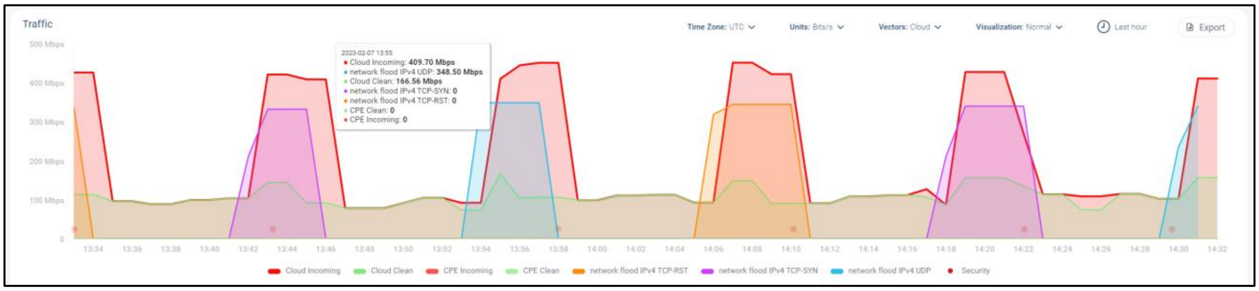
The Traffic Graph is a powerful tool that provides a clear, real-time representation of the traffic flowing in and out of our assets. It makes it simple to differentiate between legitimate and attack traffic by using distinct colors, thereby allowing for efficient monitoring of network activity and prompt identification of potential threats.

At first glance, we can see multiple peaks of traffic, these peaks are essentially attacks identified and mitigated by our cloud protection, each type of attack is marked with a different color. Our demo features a legitimate client that generates HTTP requests peaking at around 100mb, and an attacker that generates attacks peaking at around 300mb. We have 3 types of attacks as can be seen in the graph map, TCP-SYN Flood, UDP Flood, TCP-RST Flood.

Looking at the graph we have two key types of traffic, the "Cloud Incoming" shown in red, and the "Cloud Clean" displayed in green. It should be pointed out that the stability of the green "Cloud Clean" line, which remains unchanged even during an attack, indicates that legitimate traffic continues to flow uninterrupted through the cloud.

With the help of the mouse pointer, you can easily display the traffic breakdown at any point in time by hovering over the graph, making it especially useful during an attack. For example, you can observe the breakdown of a TCP-RST attack in the graph. Moreover, you can also choose to display or hide specific attack lines by interacting with the graph map.

Additionally, you can further customize the graph through the various options located in the top right corner, including Time zone, Units, Vectors, Visualizations, and Graph time. Like other sections of the portal, you can also export the graph in PDF or CSV format for more in-depth analysis.



Traffic

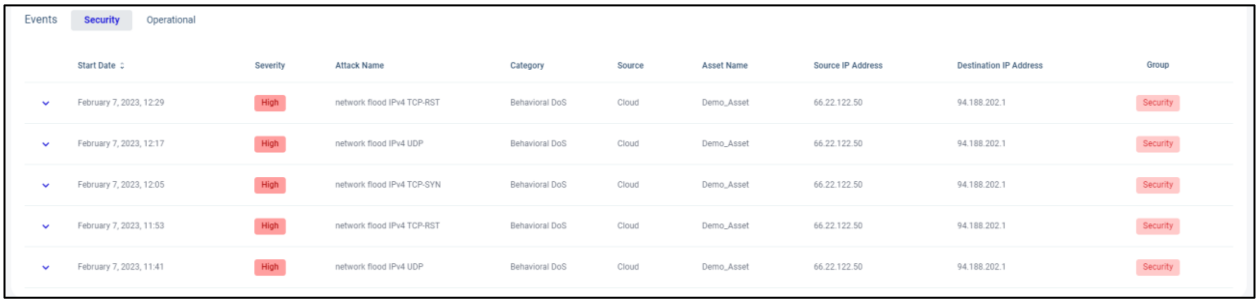
Time Zone: UTC
Units: Bits/s
Vectors: Cloud
Visualization: Normal
Last hour

2023-02-07 13:55
- Cloud Incoming: **409.70 Mbps**
- network flood IPv4 UDP: **348.50 Mbps**
- Cloud Clean: **166.56 Mbps**
- network flood IPv4 TCP-SYN: **0**
- network flood IPv4 TCP-RST: **0**
- CPE Clean: **0**
- CPE Incoming: **0**

Note: In the graph, we also have CPE Incoming & CPE Clean, however, these are relevant only for hybrid deployments, where customer uses the Cloud DDoS along with an On-Prem DefensePro.

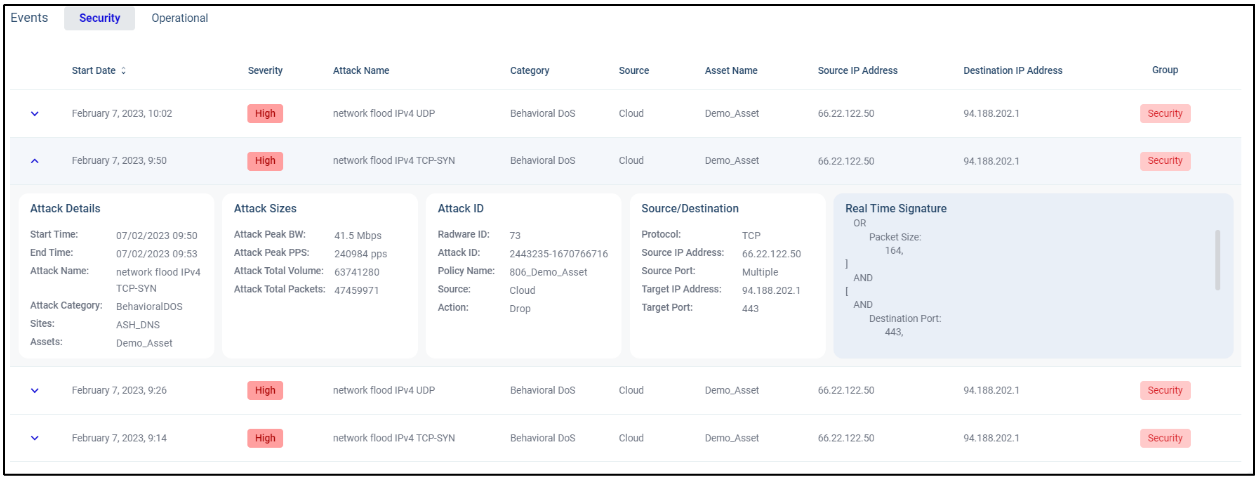
Security Events

Below the graph, we have a miniature version of the Security events, which can be accessed in full view through the left-side menu. The events displayed here correspond to the time range of the graph, making it easy to understand the events that occurred during that time.



	Start Date	Severity	Attack Name	Category	Source	Asset Name	Source IP Address	Destination IP Address	Group
⌄	February 7, 2023, 12:29	High	network flood IPv4 TCP-RST	Behavioral DoS	Cloud	Demo_Asset	66.22.122.50	94.188.202.1	Security
⌄	February 7, 2023, 12:17	High	network flood IPv4 UDP	Behavioral DoS	Cloud	Demo_Asset	66.22.122.50	94.188.202.1	Security
⌄	February 7, 2023, 12:05	High	network flood IPv4 TCP-SYN	Behavioral DoS	Cloud	Demo_Asset	66.22.122.50	94.188.202.1	Security
⌄	February 7, 2023, 11:53	High	network flood IPv4 TCP-RST	Behavioral DoS	Cloud	Demo_Asset	66.22.122.50	94.188.202.1	Security
⌄	February 7, 2023, 11:41	High	network flood IPv4 UDP	Behavioral DoS	Cloud	Demo_Asset	66.22.122.50	94.188.202.1	Security

Focusing on the security events, we can see that there are multiple alerts with a High severity, categorized as Behavioral DoS attacks. These alerts are generated by the DefensePro protection module, which is responsible for mitigating these specific types of attack, as can be seen, each attack in the graph has a corresponding event. By expanding a security alert, we can access more detailed information about the attack, including the Real-Time Signature used by the Behavioral DoS to stop the attack. As an example, below, we can see that the TCP SYN Flood attack had the following parameters: Packet Size=164, Time-to-Live=28,29,26, Destination Port=443, and Destination IP= 94.188.202.1, by utilizing these parameters, the Behavioral DoS was able to successfully block the attack without impacting the legit traffic.



	Start Date	Severity	Attack Name	Category	Source	Asset Name	Source IP Address	Destination IP Address	Group
⌄	February 7, 2023, 10:02	High	network flood IPv4 UDP	Behavioral DoS	Cloud	Demo_Asset	66.22.122.50	94.188.202.1	Security
⌃	February 7, 2023, 9:50	High	network flood IPv4 TCP-SYN	Behavioral DoS	Cloud	Demo_Asset	66.22.122.50	94.188.202.1	Security

Attack Details

Start Time:	07/02/2023 09:50
End Time:	07/02/2023 09:53
Attack Name:	network flood IPv4 TCP-SYN
Attack Category:	BehavioralDOS
Sites:	ASH_DNS
Assets:	Demo_Asset

Attack Sizes

Attack Peak BW:	41.5 Mbps
Attack Peak PPS:	240984 pps
Attack Total Volume:	63741280
Attack Total Packets:	47459971

Attack ID

Radware ID:	73
Attack ID:	2443235-1670766716
Policy Name:	806_Demo_Asset
Source:	Cloud
Action:	Drop

Source/Destination

Protocol:	TCP
Source IP Address:	66.22.122.50
Source Port:	Multiple
Target IP Address:	94.188.202.1
Target Port:	443

Real Time Signature

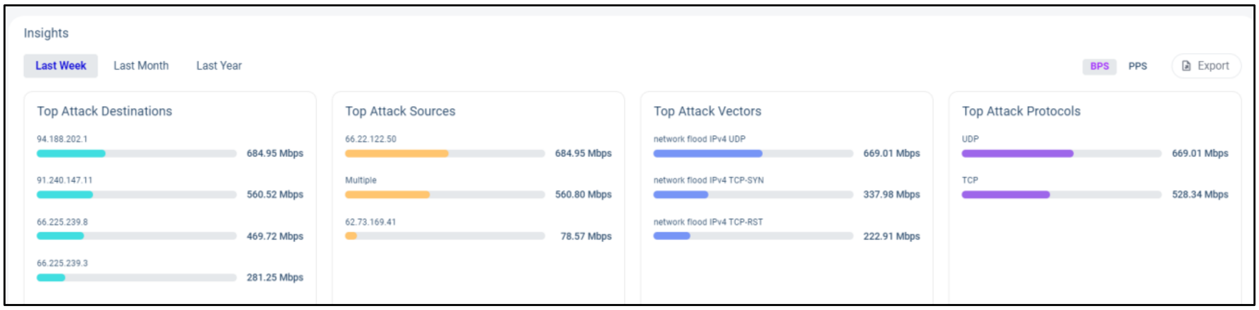
```
 OR
     Packet Size:
         164,
]
 AND
[
 AND
     Destination Port:
         443,
```

	Start Date	Severity	Attack Name	Category	Source	Asset Name	Source IP Address	Destination IP Address	Group
⌄	February 7, 2023, 9:26	High	network flood IPv4 UDP	Behavioral DoS	Cloud	Demo_Asset	66.22.122.50	94.188.202.1	Security
⌄	February 7, 2023, 9:14	High	network flood IPv4 TCP-SYN	Behavioral DoS	Cloud	Demo_Asset	66.22.122.50	94.188.202.1	Security

Insights

The last section of the overview page, Insights, provides a comprehensive overview of the attacks on our protected assets. This view offers a broader perspective, with a larger timeframe than the real-time graph shown in the previous section, giving us a deeper understanding of the attack landscape, trends, and patterns.

The graphs can be displayed in either Bits per second or Packets per second, providing flexibility in the unit of measurement that best suits the user's needs. Additionally, the information can be exported to a PDF or CSV file for further analysis, similar to other sections of the portal.



Top Attack Destinations	
94.188.202.1	684.95 Mbps
91.240.147.11	560.52 Mbps
66.225.239.8	469.72 Mbps
66.225.239.3	281.25 Mbps

Top Attack Sources	
66.22.122.50	684.95 Mbps
Multiple	560.80 Mbps
62.73.169.41	78.57 Mbps

Top Attack Vectors	
network flood IPv4 UDP	669.01 Mbps
network flood IPv4 TCP-SYN	337.98 Mbps
network flood IPv4 TCP-RST	222.91 Mbps

Top Attack Protocols	
UDP	669.01 Mbps
TCP	528.34 Mbps

Security Events

Action:

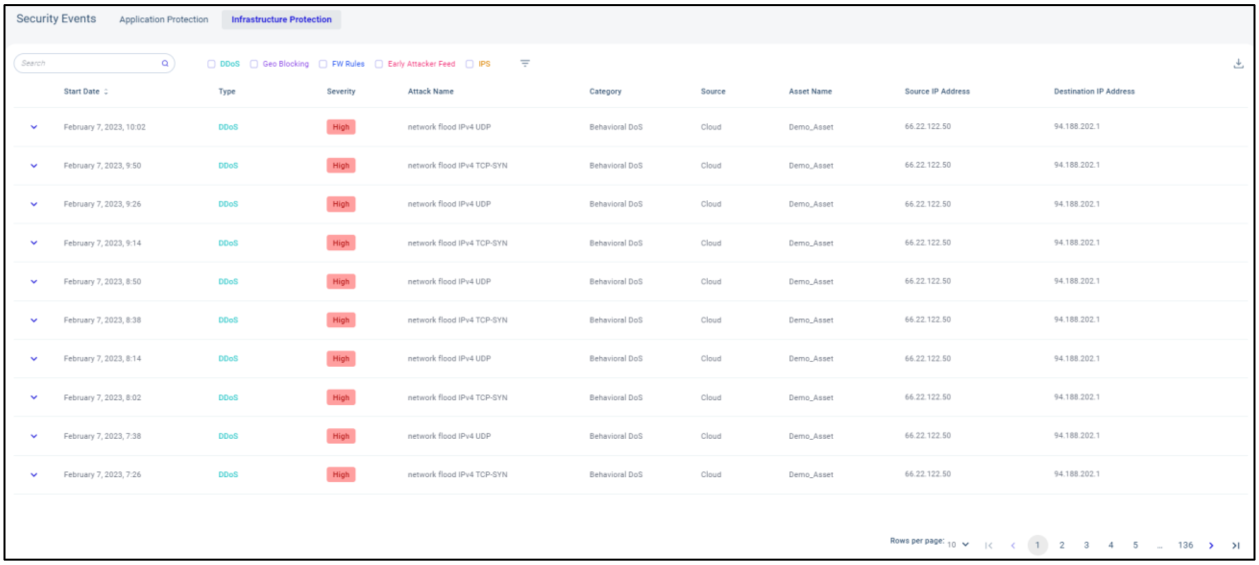
1. Select the Security Events from the left sidebar. Make sure the Infrastructure Protection button is pressed, not the Application Protection button.
2. Explain how this page is different from the real-time view seen in the Overview section.
3. Show the capability to filter by category and severity.

Description:

As discussed in the Overview section, The Security Events menu provides detailed information on all security-related incidents that have occurred on our assets. Unlike the real-time graph and events displayed in the previous section, this menu provides a log-based view of the security incidents, giving us a broader understanding of the attack landscape and trends over time.

The log can be searched for specific events using the search bar and filtered based on different parameters using the filter button ☰ , as well as downloaded for further analysis. Furthermore, this section has a quick filtering pane based on attack categories like DDoS, Geo Blocking, FW Rules, Early Attacker Feed and IPS. Please note that in our demo we only have DDoS based attack scenarios.

As we saw in the Overview section, we can expand each event to gain deeper insights into the attack characteristics including the real time signature that was used to mitigate it.



□ DDoS □ Geo Blocking □ FW Rules □ Early Attacker Feed □ IPS

	Start Date	Type	Severity	Attack Name	Category	Source	Asset Name	Source IP Address	Destination IP Address
⌄	February 7, 2023, 10:02	DDoS	High	network flood IPv4 UDP	Behavioral DoS	Cloud	Demo_Asset	66.22.122.50	94.188.202.1
⌄	February 7, 2023, 9:50	DDoS	High	network flood IPv4 TCP-SYN	Behavioral DoS	Cloud	Demo_Asset	66.22.122.50	94.188.202.1
⌄	February 7, 2023, 9:26	DDoS	High	network flood IPv4 UDP	Behavioral DoS	Cloud	Demo_Asset	66.22.122.50	94.188.202.1
⌄	February 7, 2023, 9:14	DDoS	High	network flood IPv4 TCP-SYN	Behavioral DoS	Cloud	Demo_Asset	66.22.122.50	94.188.202.1
⌄	February 7, 2023, 8:50	DDoS	High	network flood IPv4 UDP	Behavioral DoS	Cloud	Demo_Asset	66.22.122.50	94.188.202.1
⌄	February 7, 2023, 8:38	DDoS	High	network flood IPv4 TCP-SYN	Behavioral DoS	Cloud	Demo_Asset	66.22.122.50	94.188.202.1
⌄	February 7, 2023, 8:14	DDoS	High	network flood IPv4 UDP	Behavioral DoS	Cloud	Demo_Asset	66.22.122.50	94.188.202.1
⌄	February 7, 2023, 8:02	DDoS	High	network flood IPv4 TCP-SYN	Behavioral DoS	Cloud	Demo_Asset	66.22.122.50	94.188.202.1
⌄	February 7, 2023, 7:38	DDoS	High	network flood IPv4 UDP	Behavioral DoS	Cloud	Demo_Asset	66.22.122.50	94.188.202.1
⌄	February 7, 2023, 7:26	DDoS	High	network flood IPv4 TCP-SYN	Behavioral DoS	Cloud	Demo_Asset	66.22.122.50	94.188.202.1

Rows per page: 10 ⌄ |< < 1 2 3 4 5 ... 136 > >|

Analytics

Actions:

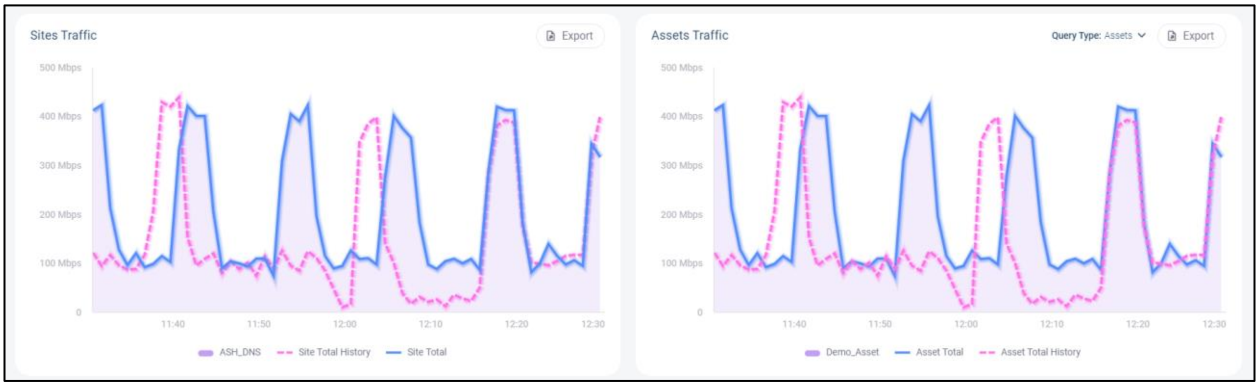
1. Select Analytics from the left side menu.
2. Explain this is an Add-On service.
3. Discuss the value of analytics.
4. Explain and how it can be used even when an asset is off cloud.
5. Explain the graph data points difference in relation to real time graph.
6. Go through each widget:
   a. Graph view of Sites and Assets, explain the Asset Total & Asset Total History.
   b. Top source by country.
   c. Top services.
   d. Top source IP addresses.
   e. Top conversations.

Description:

The Analytics section is an Add-On service that provides customers with valuable insights into their network traffic. Unlike the Real-Time graph, which averages traffic as you look back in time, Analytics provides an accurate and in-depth view of a customer's network traffic by utilizing data points spanning up to 3 months. This is accomplished by the use of a multi-widget screen, where each widget provides a different view of the traffic, allowing for a more comprehensive grasp of te situation. Overall, the Analytics section is a powerful tool that enables customers to gain a deeper understanding of their network traffic and make data-driven decisions.

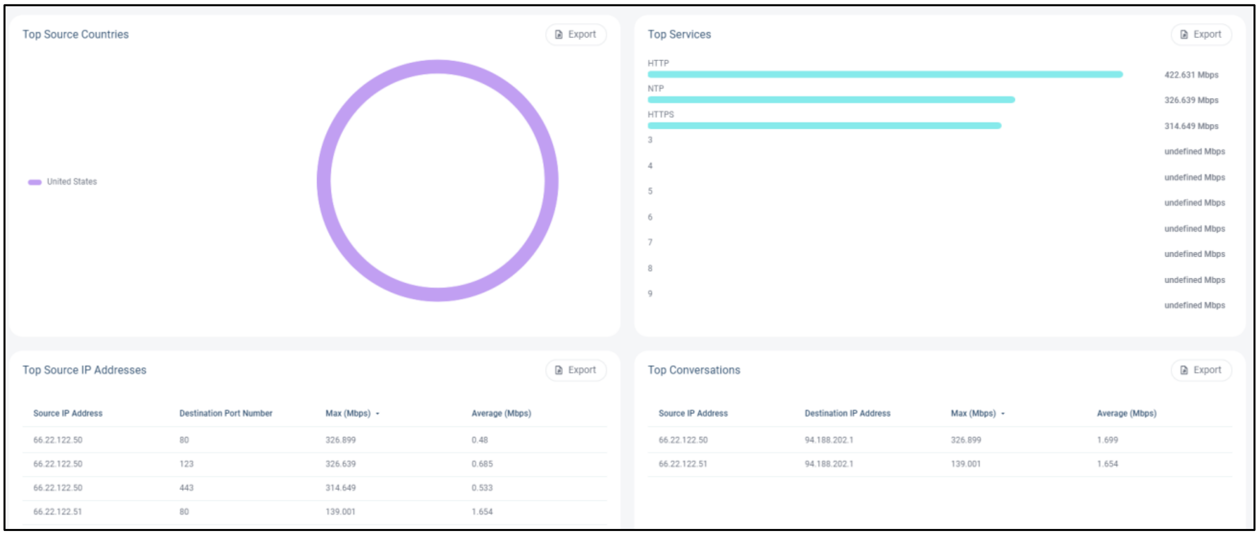
The top section of the page offers a wide range of options for manipulating the presented information, such as viewing analytics for specific assets, sites, and time ranges, as well as the ability to view traffic from the cloud or CPE origin (using NetFlow sent from customer routers). Additionally, customers can choose the type of aggregation they wish to use, such as maximum or average.

In our demo we will start by looking at the Site and Asset Traffic Graphs. As can be seen in our case, we display identical traffic as we only have one active asset in one site. Looking at the graph map, we can see two important features: Site Total and Site Total History. Site Total displays the total traffic for the chosen time range, while Site Total History provides a historical view for the same time range, for comparison: for example, if the chosen time range is 1 month, Site Total History will provide an overlapping view for the prior month. Additionally, customers also have the option to select a custom time range by interacting with the graph to select a specific portion to zoom into, allowing for a more accurate analysis.



The Asset graph allows customers to view network traffic data in a more granular way by providing two query types: Assets and Addresses, **Query Type:** Assets ⌄ Export this allows customers to view traffic data grouped by specific assets or by individual addresses. However, note that this feature is limited to displaying data for up to 20 assets or addresses in the graph at a time.

Customers can also gain insight into the geographical distribution of their network traffic with the Top Sources Countries graph. Additionally, they can view the most frequently used services, top source IP addresses, and top conversations.



Top Source IP Addresses

Source IP Address	Destination Port Number	Max (Mbps) ▾	Average (Mbps)
66.22.122.50	80	326.899	0.48
66.22.122.50	123	326.639	0.685
66.22.122.50	443	314.649	0.533
66.22.122.51	80	139.001	1.654

Top Conversations

Source IP Address	Destination IP Address	Max (Mbps) ▾	Average (Mbps)
66.22.122.50	94.188.202.1	326.899	1.699
66.22.122.51	94.188.202.1	139.001	1.654

Notifications

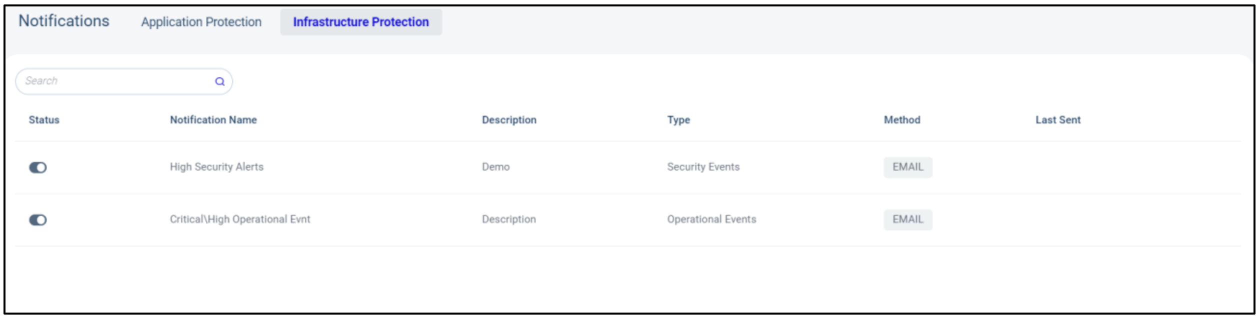
Actions:

1. Select Notifications from the left side menu.
2. Highlight the value of notifications.
3. Show the existing security & operational notifications and explain their configuration.

Description:

The Notifications section in the portal allows customers to stay informed on important events happening in their network. In this section, customers can configure two types of notifications: Security Events and Operational Events. The notifications can be configured to be triggered based on predefined severity levels such as High or Critical, attack rate and more. In addition, customers can choose to receive notifications via email or SMS.

In our demo, we have preconfigured a Security Event notification with High severity to be sent when an attack is above 100Mbps via email, We have also preconfigured an Operational Event notification to be sent when Critical and High Severity events are invoked which can include On-Cloud and Off-Cloud events relevant for On-Demand Customers, GRE tunnel status and more.



Status	Notification Name	Description	Type	Method	Last Sent
●	High Security Alerts	Demo	Security Events	EMAIL	
●	Critical\High Operational Evnt	Description	Operational Events	EMAIL	

Reports

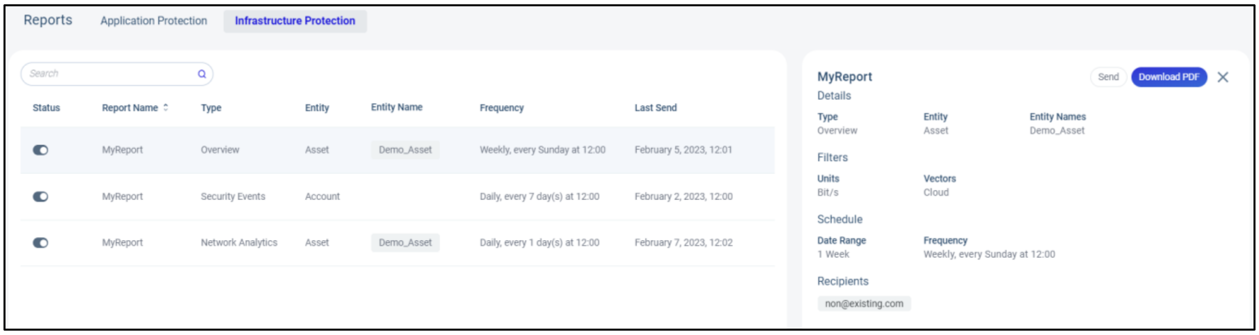
Actions:

1. Select Reports from the left side menu.
2. Discuss the value of reports.
3. Explain existing types of reports.
4. Download an "Overview" type report to show its contents.

Description:

The Reports Section of the portal allows customers to create reports that can be scheduled to be sent at regular intervals. The three types of reports available are Overview, Security Events, and Analytics. These reports provide a comprehensive view of the customer's network and security status and can be used to track trends and identify areas for improvement.

In our demo we have created three predefined reports. By clicking on each report, a new window will open where you can download and open the report in order to present the content that will be sent via email at predefined intervals.



Status	Report Name	Type	Entity	Entity Name	Frequency	Last Send
●	MyReport	Overview	Asset	Demo_Asset	Weekly, every Sunday at 12:00	February 5, 2023, 12:01
●	MyReport	Security Events	Account		Daily, every 7 day(s) at 12:00	February 2, 2023, 12:00
●	MyReport	Network Analytics	Asset	Demo_Asset	Daily, every 1 day(s) at 12:00	February 7, 2023, 12:02

MyReport

Details

Type: Overview
Entity: Asset
Entity Names: Demo_Asset

Filters

Units: Bit/s
Vectors: Cloud

Schedule

Date Range: 1 Week
Frequency: Weekly, every Sunday at 12:00

Recipients

non@existing.com