Network Insights

Belden Horizon

June 5, 2024

USER MANUAL

Your Feedback Please

We always want you to feel that you made the right decision to use our products. If you have suggestions, comments, compliments or complaints about our products, documentation, or support, please write or call us.

ProSoft Technology, Inc.
+1 (661) 716-5100
+1 (661) 716-5101 (Fax)
www.prosoft-technology.com
support@prosoft-technology.com

Belden Horizon Network Insights User Manual
For Public Use.

June 5, 2024

Content Disclaimer

This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation, and testing of the products with respect to the relevant specific application or use thereof. Neither ProSoft Technology nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. Information in this document including illustrations, specifications and dimensions may contain technical inaccuracies or typographical errors. ProSoft Technology makes no warranty or representation as to its accuracy and assumes no liability for and reserves the right to correct such inaccuracies or errors at any time without notice. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without express written permission of ProSoft Technology. All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components. When devices are used for applications with technical safety requirements, the relevant instructions must be followed. Failure to use ProSoft Technology software or approved software with our hardware products may result in injury, harm, or improper operating results. Failure to observe this information can result in injury or equipment damage.

Open Source Information

Open Source Software used in the product

The product contains, among other things, Open Source Software files, as defined below, developed by third parties and licensed under an Open Source Software license. These Open Source Software files are protected by copyright. Your right to use the Open Source Software is governed by the relevant applicable Open Source Software license conditions. Your compliance with those license conditions will entitle you to use the Open Source Software as foreseen in the relevant license. In the event of conflicts between other ProSoft Technology, Inc. license conditions applicable to the product and the Open Source Software license conditions, the Open Source Software conditions shall prevail. The Open Source Software is provided royalty-free (i.e. no fees are charged for exercising the licensed rights). Open Source Software contained in this product and the respective Open Source Software licenses are stated in the module webpage, in the link Open Source.

If Open Source Software contained in this product is licensed under GNU General Public License (GPL), GNU Lesser General Public License (LGPL), Mozilla Public License (MPL) or any other Open Source Software license, which requires that source code is to be made available and such source code is not already delivered together with the product, you can order the corresponding source code of the Open Source Software from ProSoft Technology, Inc. - against payment of the shipping and handling charges - for a period of at least 3 years since purchase of the product. Please send your specific request, within 3 years of the purchase date of this product, together with the name and serial number of the product found on the product label to:

ProSoft Technology, Inc.
Director of Engineering
9201 Camino Media, Suite 200
Bakersfield, CA 93311
USA

Warranty regarding further use of the Open Source Software

ProSoft Technology, Inc. provides no warranty for the Open Source Software contained in this product, if such Open Source Software is used in any manner other than intended by ProSoft Technology, Inc. The licenses listed below define the warranty, if any, from the authors or licensors of the Open Source Software. ProSoft Technology, Inc. specifically disclaims any warranty for defects caused by altering any Open Source Software or the product's configuration. Any warranty claims against ProSoft Technology, Inc. in the event that the Open Source Software contained in this product infringes the intellectual property rights of a third party are excluded. The following disclaimer applies to the GPL and LGPL components in relation to the rights holders:

"This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License and the GNU Lesser General Public License for more details."

For the remaining open source components, the liability exclusions of the rights holders in the respective license texts apply. Technical support, if any, will only be provided for unmodified software.

Table of Contents

1 Start Here

1.1 About BHNI

Wherever individual network components combine to form a comprehensive system, Belden Horizon Network Insights (BHNI) becomes the ideal solution for configuring and monitoring administrable Belden devices such as switches, routers, OpEdge-8D firewalls, as well as wireless BAT units and products from various manufacturers. BHNI, designed for efficient industrial supervision, can seamlessly integrate into the network. Using machine-learning algorithms, BHNI analyses network behavior over time and detects anomalies, offering insights into network traffic patterns to help identify anomalies.

2 Belden Horizon Registration

The device must be registered in Belden Horizon before installing the Container on the device. To register, follow the steps in Chapter 3 of the OpEdge Configuration document.

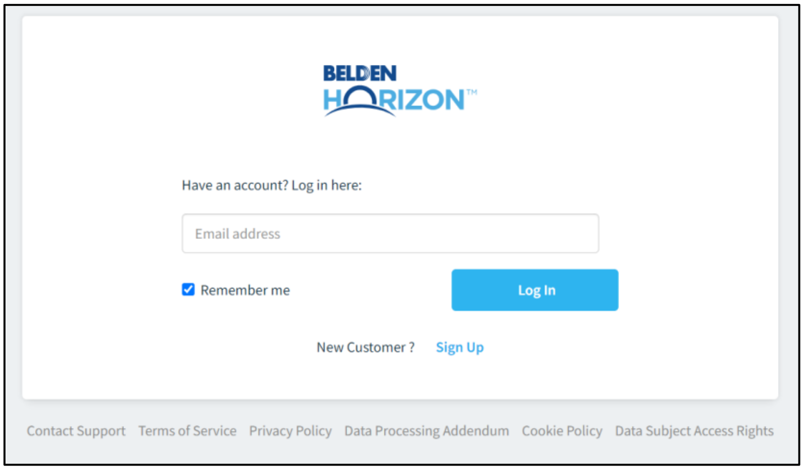
Once the device is successfully registered, continue with the steps in the following chapter.

3 Container Installation and Deployment

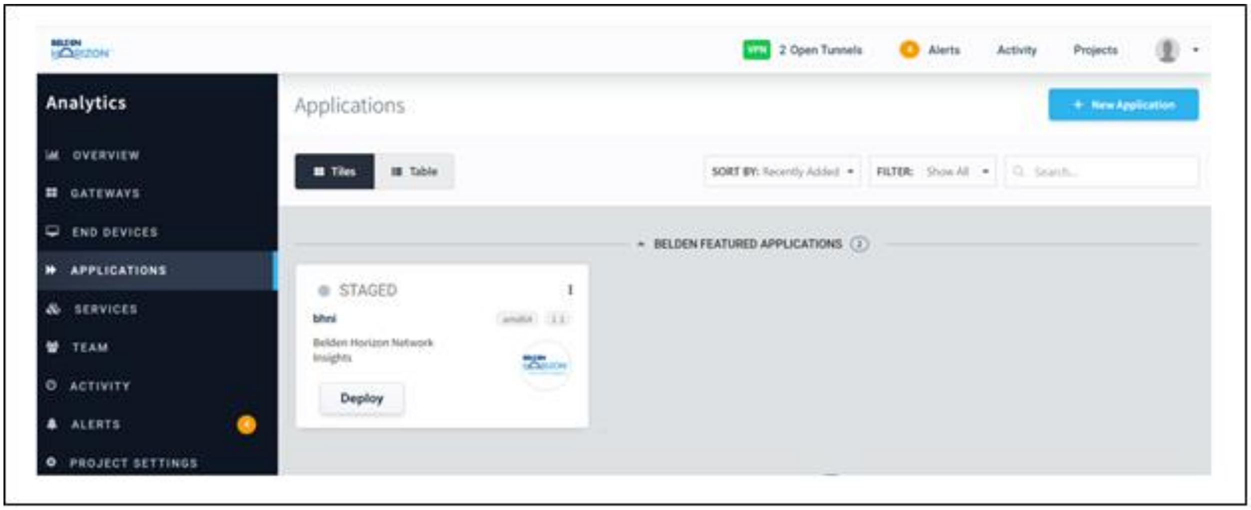
Perform the following steps for the installation and deployment of containers.

1 Open the website https://belden.io.

2 Log in to your account. If you do not have an account, click the **SIGNUP** button to create an account. The **Overview** page displays after successful login.



3 Click on **APPLICATIONS** in the left panel. Scroll-down to the **bhni** container.

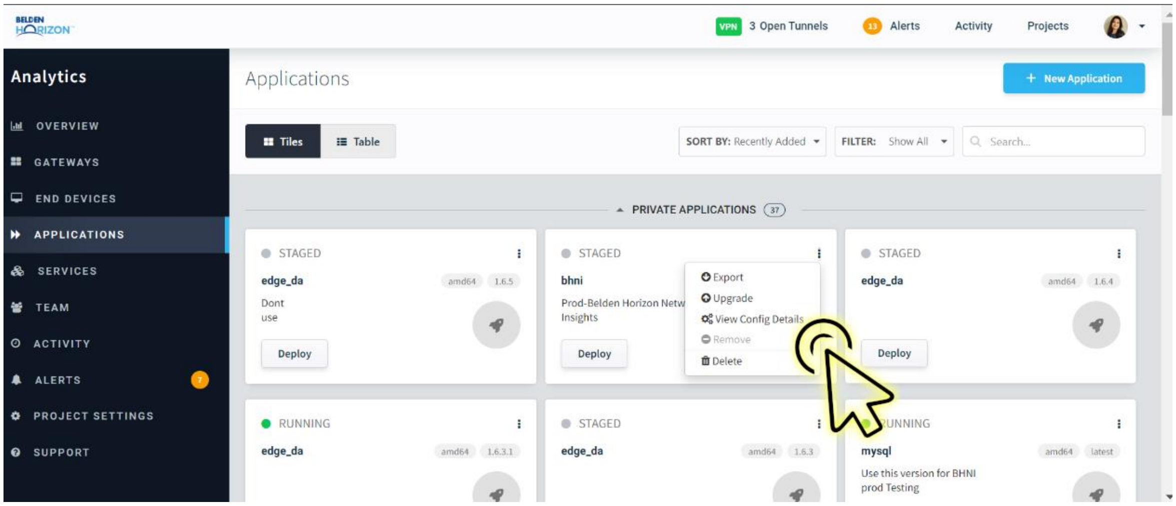


The following section covers the deployment of a container.

3.1 Deploying bhni Container

The **bhni** container is required for viewing live data. Perform the following steps to deploy the **bhni** container:

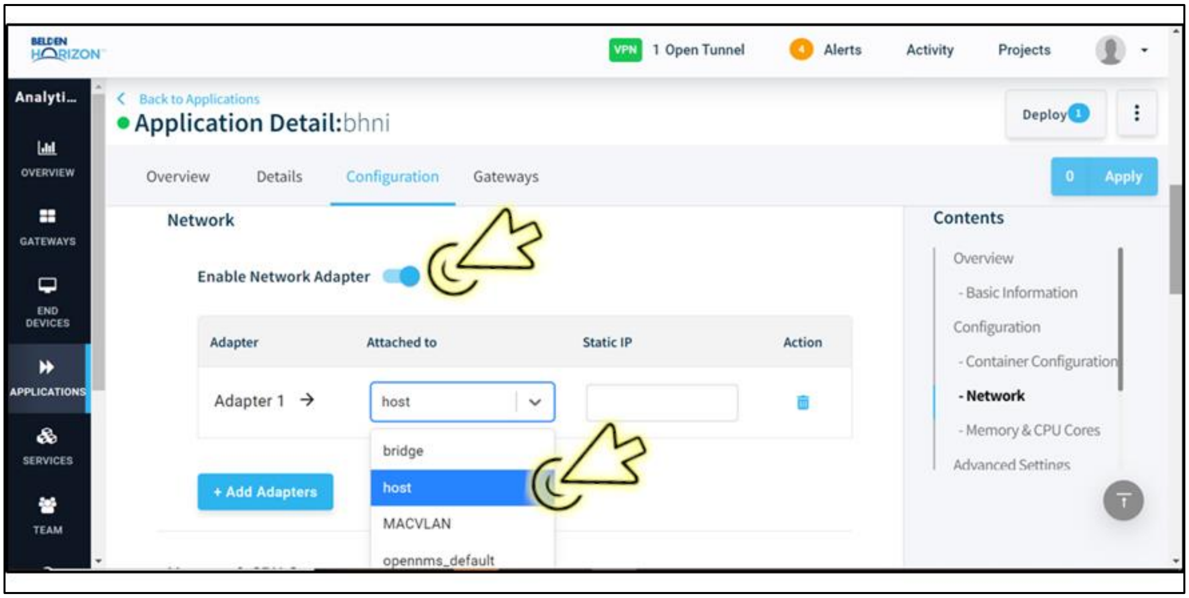
1 In the **bhni** container options, select **VIEW CONFIG DETAILS** to open the *Application Detail* page.



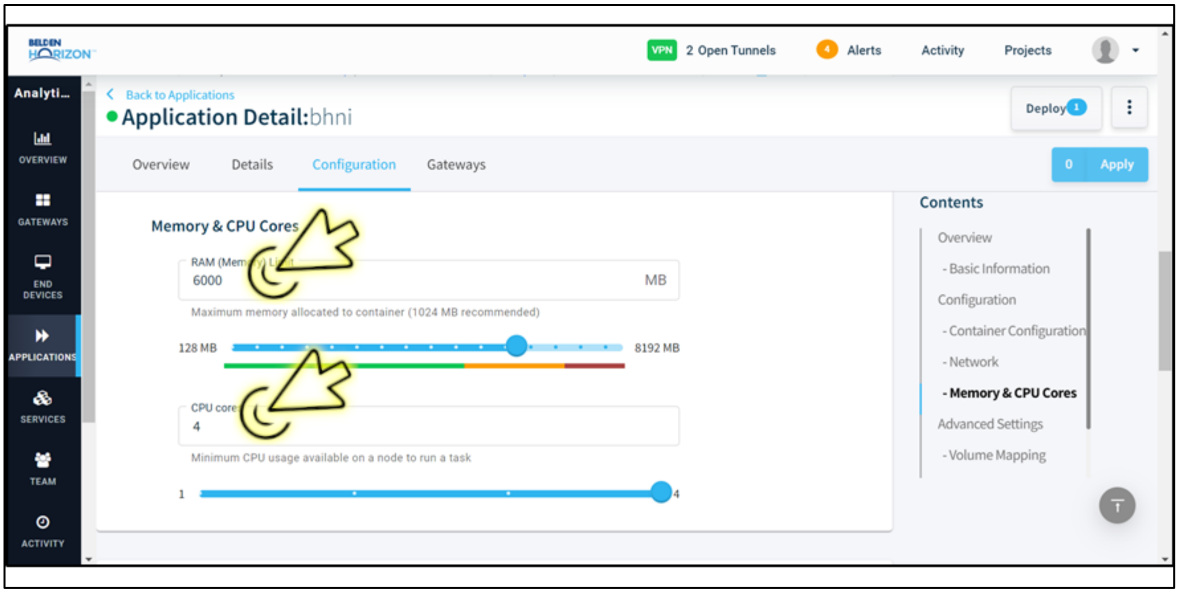
2 In the *Configuration* tab of the *Application Detail* page, scroll down to the **Network** section.

a) Enable the **ENABLE NETWORK ADAPTER** toggle button.

b) Select **HOST** from the **ATTACHED TO** drop-down list for *Adapter 1.*



3 Scroll down to **Memory & CPU Cores** frame. Specify the required values for the *RAM (Memory) Limit* and *CPU cores*.



Application Detail:bhni

Memory & CPU Cores

RAM (Mem... L... 6000 MB

Maximum memory allocated to container (1024 MB recommended)

128 MB 8192 MB

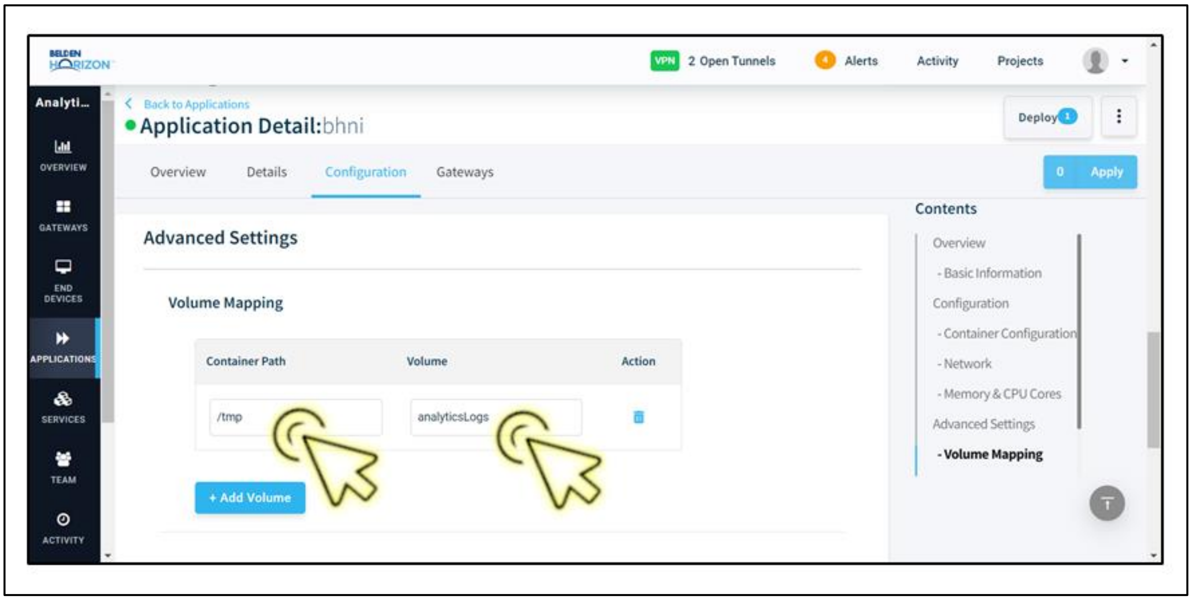
CPU core... 4

Minimum CPU usage available on a node to run a task

1 4

4 Scroll down to **Advanced Settings** frame. Specify the required values for the *Container Path* and *Volume* fields.

- **Container path**: /tmp
- **Volume**: analyticsLogs



Application Detail:bhni

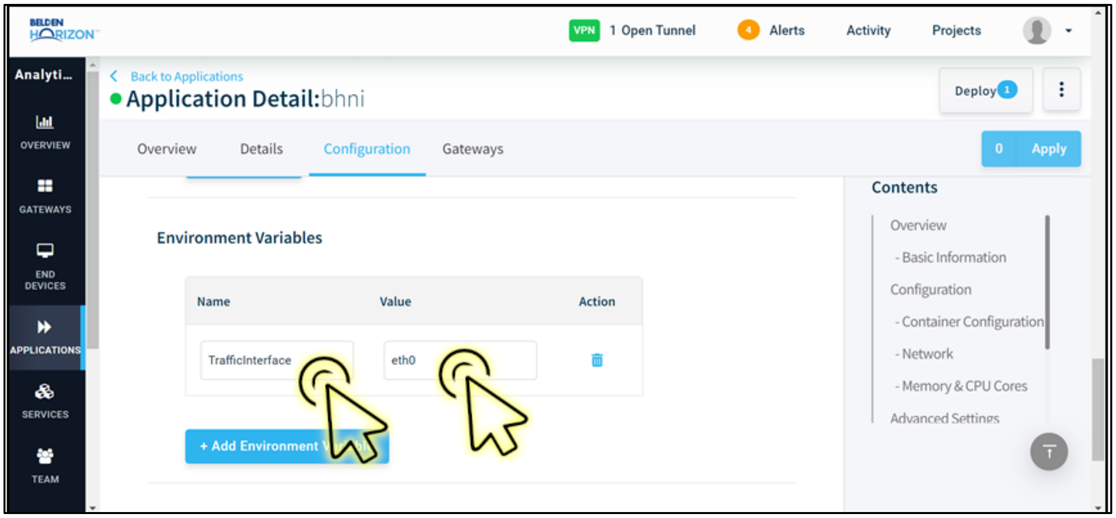
Advanced Settings

Volume Mapping

Container Path	Volume	Action
/tmp	analyticsLogs	

5 Scroll down to the *Environment Variables* section. Specify the required values for the *Name* and *Value* fields.

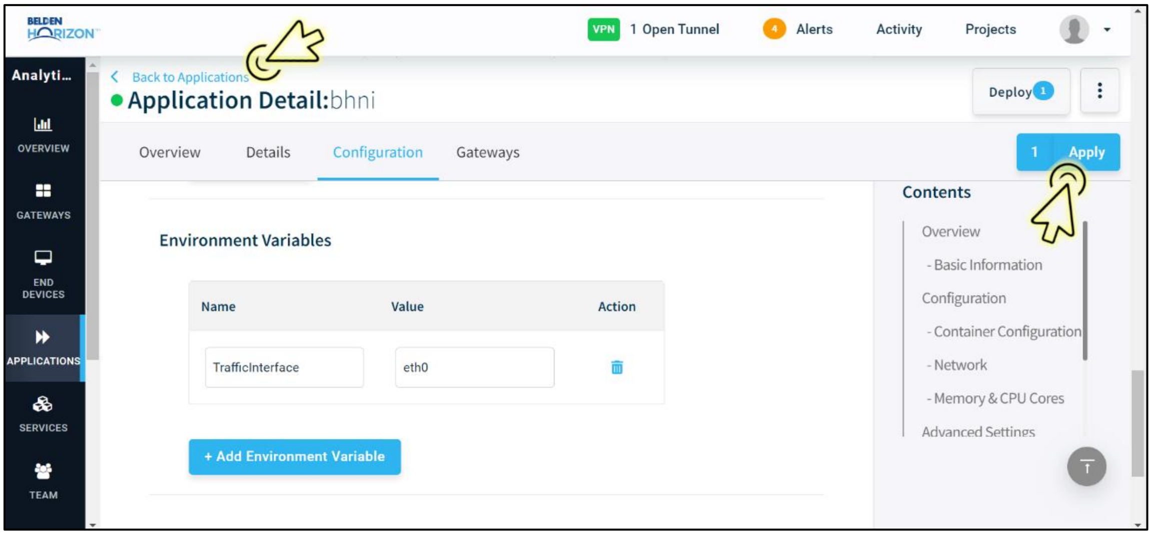
- **Name**: TrafficInterface
- **Volume**: eth0



Environment Variables

Name	Value	Action
TrafficInterface	eth0	🗑

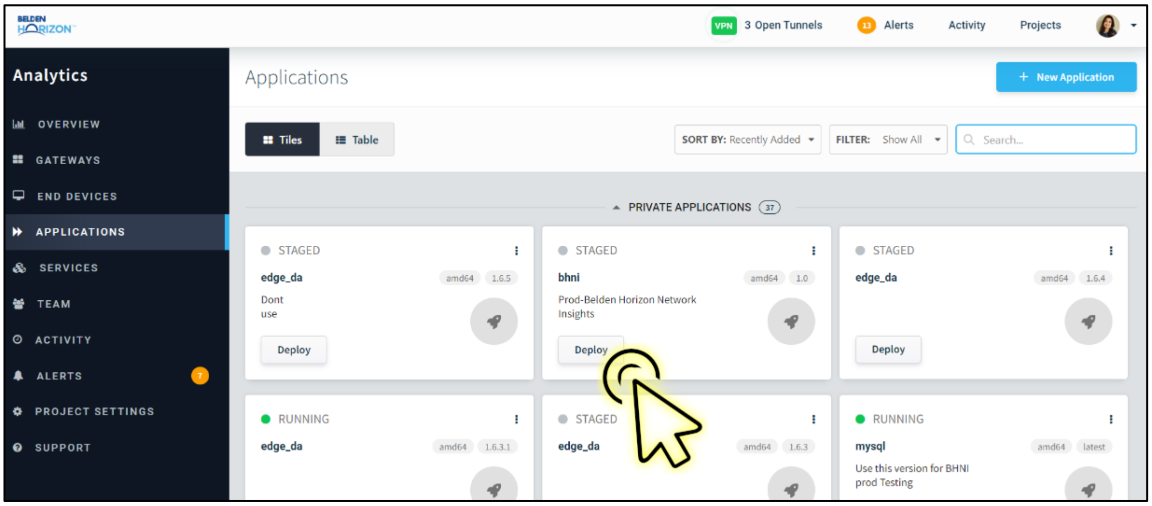
6 Click on the **Apply** button to save the changes, then click on **Back to Applications**.



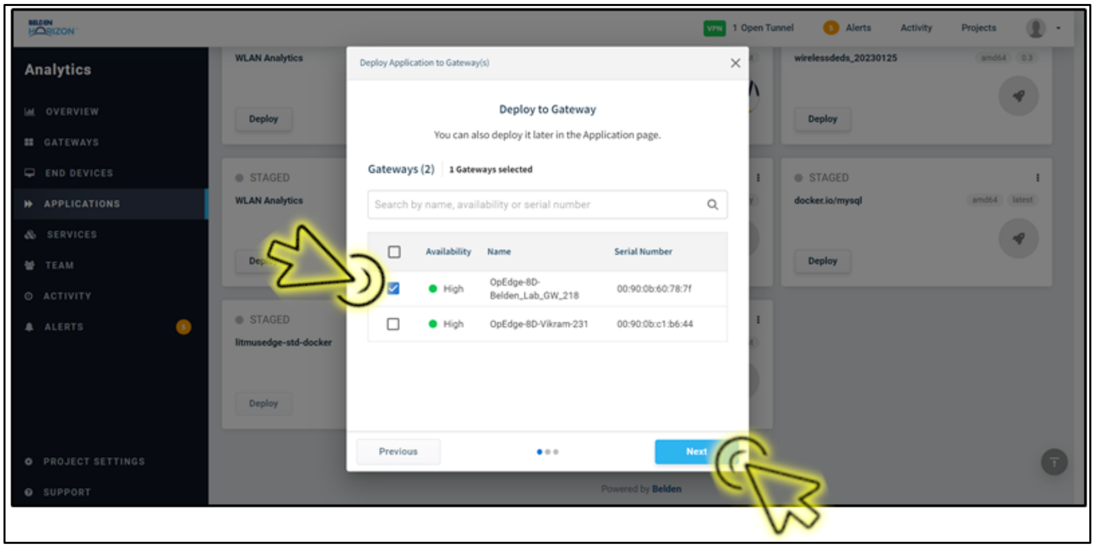
Environment Variables

Name	Value	Action
TrafficInterface	eth0	🗑

7 Click on the **DEPLOY** button to open the *Deploy Application to Gateway(s)* window.



8 Select the gateway, then click on the **NEXT** button.



Deploy Application to Gateway(s)

Deploy to Gateway

You can also deploy it later in the Application page.

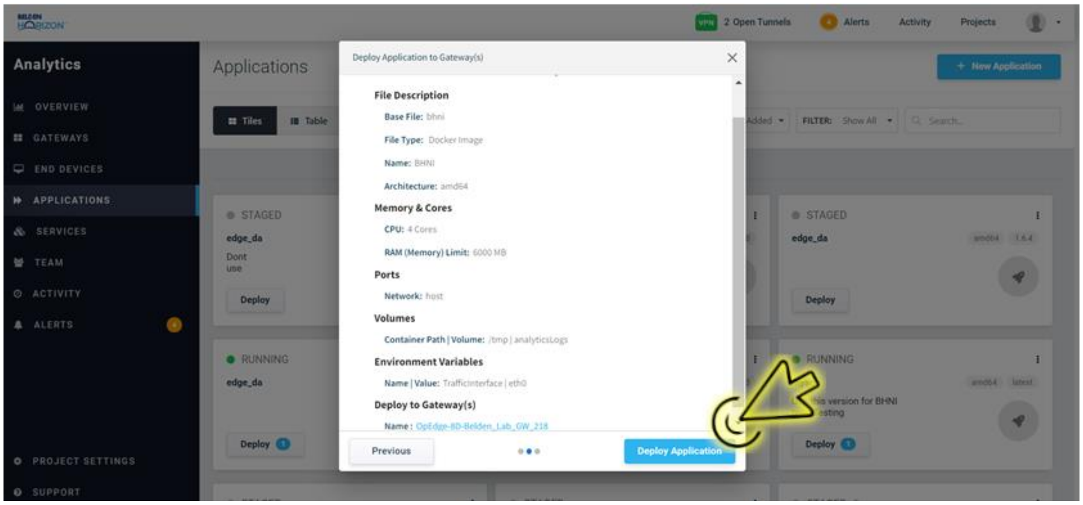
Gateways (2) 1 Gateways selected

Search by name, availability or serial number

□	Availability	Name	Serial Number
☑	● High	OpEdge-8D-Belden_Lab_GW_218	00:90:0b:60:78:7f
□	● High	OpEdge-8D-Vikram-231	00:90:0b:c1:b6:44

Previous Next

9 Verify the information is correct, then click on the **DEPLOY APPLICATION** button.



Deploy Application to Gateway(s)

File Description

Base File: bhni

File Type: Docker Image

Name: BHNI

Architecture: amd64

Memory & Cores

CPU: 4 Cores

RAM (Memory) Limit: 6000 MB

Ports

Network: host

Volumes

Container Path | Volume: /tmp | analyticsLogs

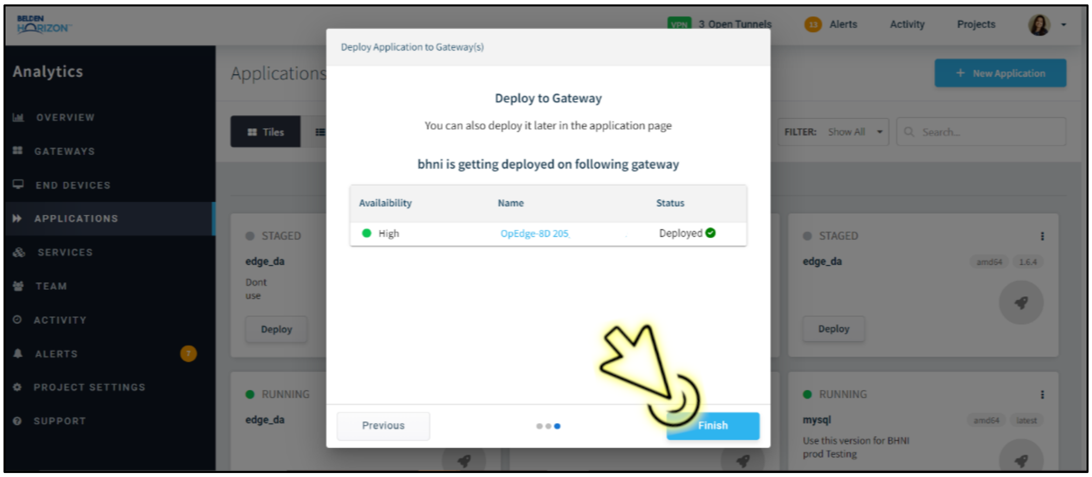
Environment Variables

Name | Value: TrafficInterface | eth0

Deploy to Gateway(s)

Name : OpEdge-8D-Belden_Lab_GW_218

10 Wait for a few seconds until the Status changes to **DEPLOYED**, then click on the **FINISH** button.



Deploy Application to Gateway(s)

Deploy to Gateway

You can also deploy it later in the application page

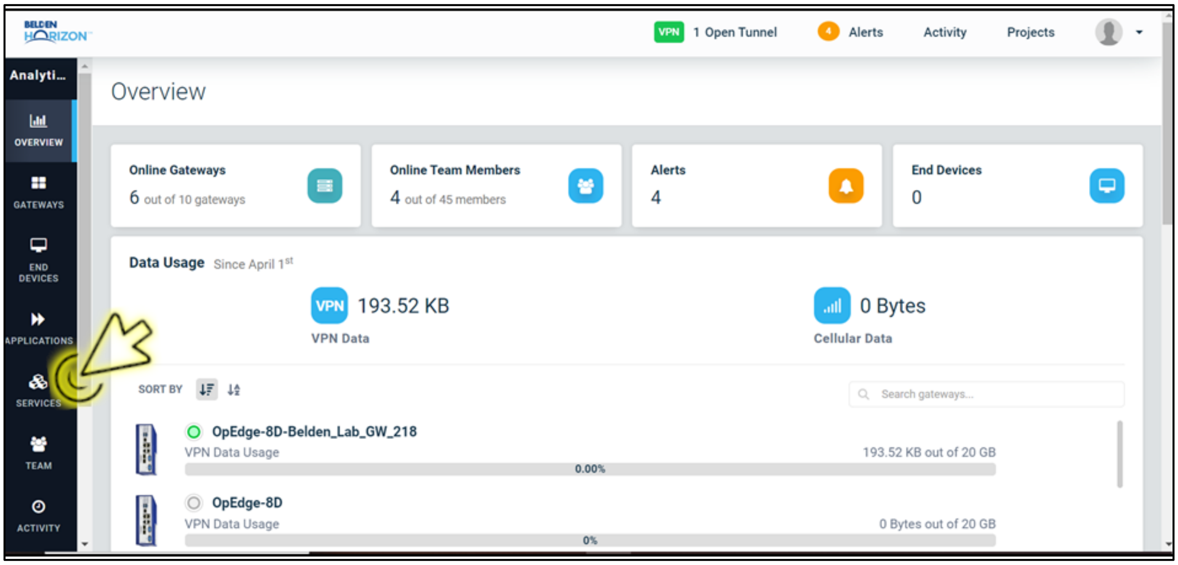
bhni is getting deployed on following gateway

Availaibility	Name	Status
● High	OpEdge-8D 205	Deployed ✓

4 Network Insights

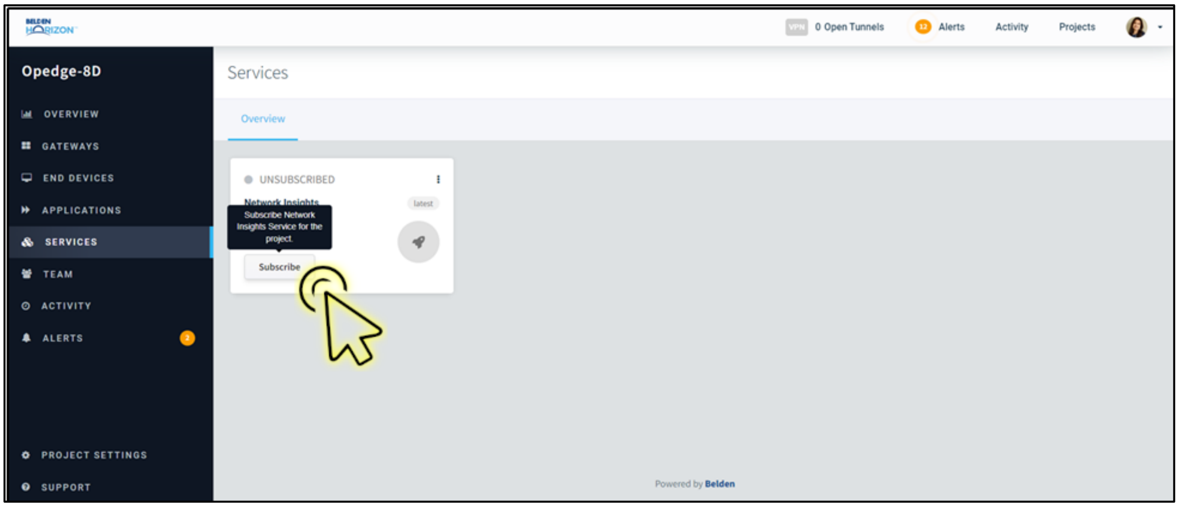
After the container installation is complete, the user can access the Network Insights for the devices registered on Belden Horizon. BHNI provides actionable network insights based on the network data gathered through passive sniffing of the captured packets. To access, perform following steps:

1. Open the website https://belden.io and log in.
2. Click on **SERVICES** in the left panel.



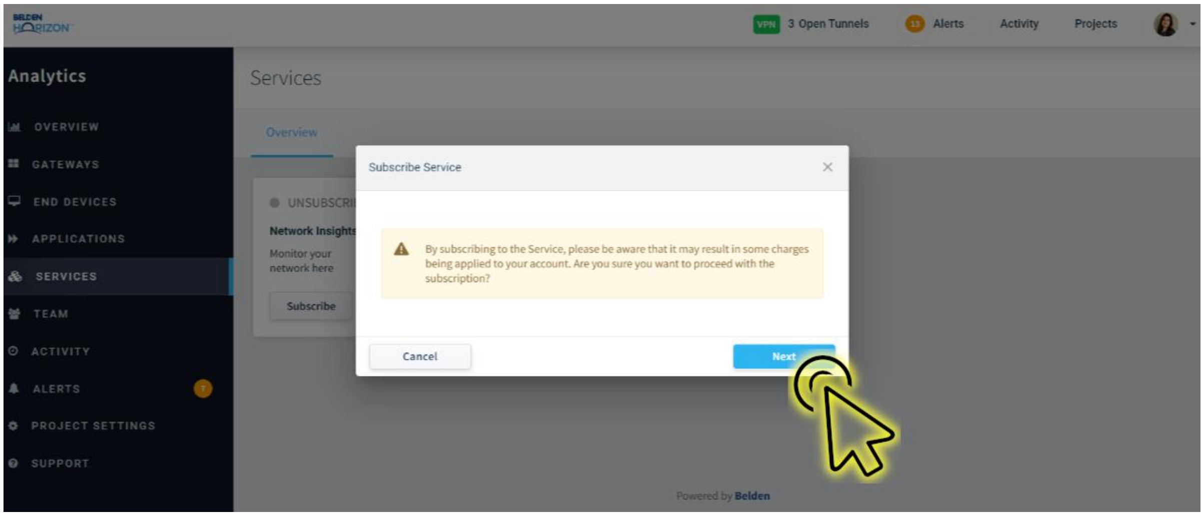
3. The **Network Insights** card is located in the *Overview* tab. Click the **SUBSCRIBE** button to open the Belden Horizon support pop-up.

> **Note:** The **Admin** user can only perform the subscribing of the Network Insight service.



4 After Belden Support provides a subscription for the account, click the **SUBSCRIBE** button again to open the *Subscribe Service* window.

5 Click the **NEXT** button to open the End User License Agreement (EULA) page.



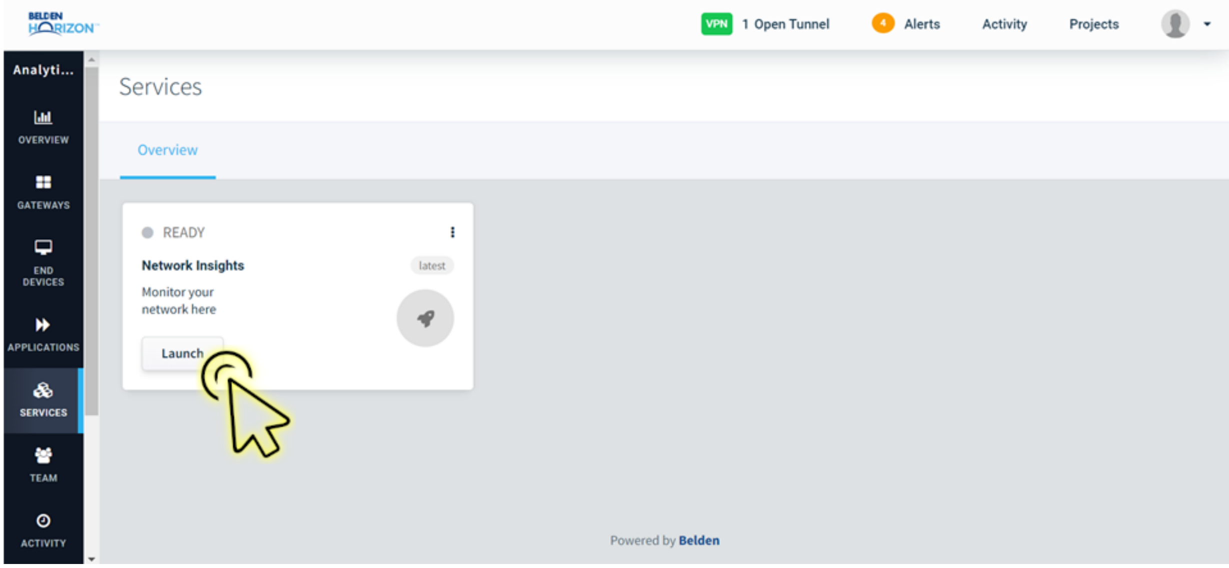
Subscribe Service

By subscribing to the Service, please be aware that it may result in some charges being applied to your account. Are you sure you want to proceed with the subscription?

6 Click the **ACCEPT & SUBSCRIBE** button.

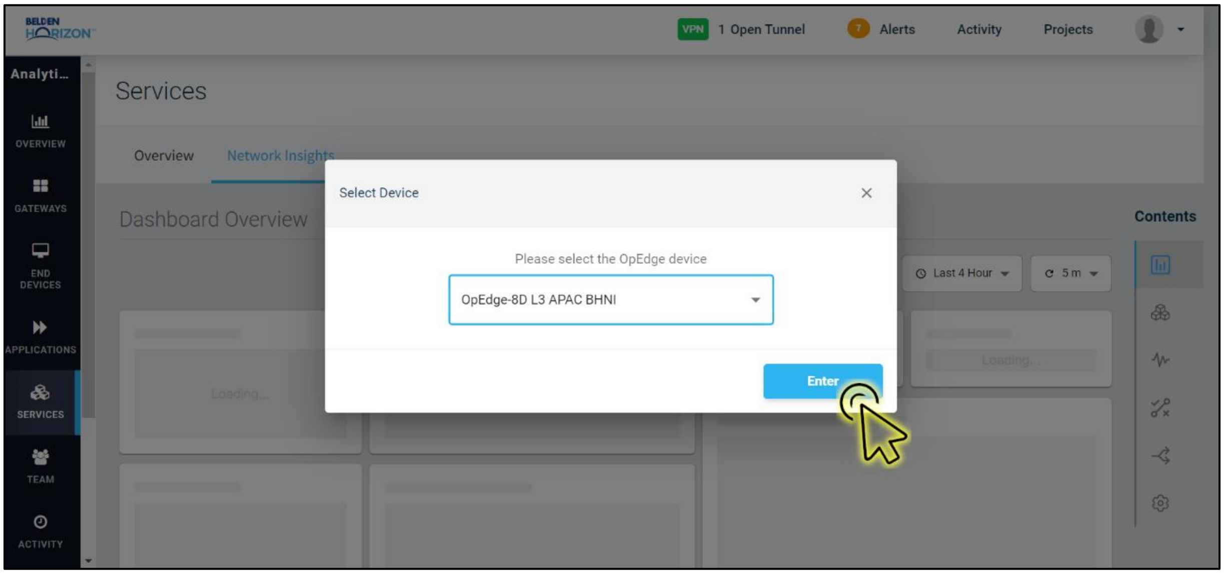
7 After subscribing, the **SUBSCRIBE** button changes to **LAUNCH**. Now any authorized user can view *Network Insights*.

8 Click the **LAUNCH** button to open a window to select the device.



9 All the registered devices on Belden Horizon will be available in the drop-down list. Select the device for which you want to view the insights and then click on **ENTER**.

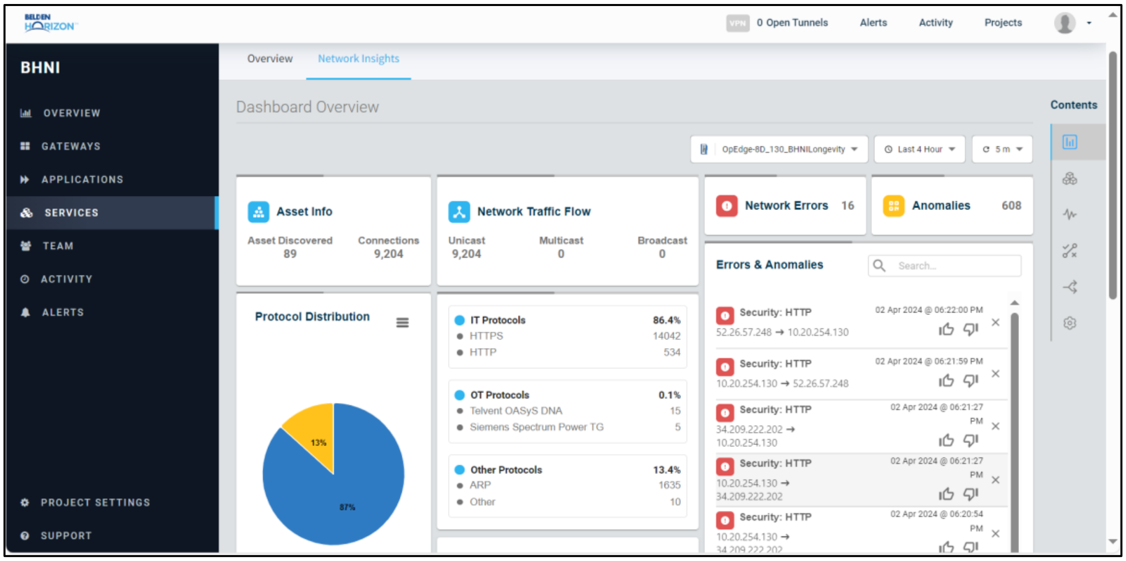
As a prerequisite, you must deploy the containers for the device selected from the drop-down list.



Please select the OpEdge device

OpEdge-8D L3 APAC BHNI

10 The *Dashboard Overview* is displayed in the *Network Insights* tab. There are different types of menus available in the **Contents** panel on the right side of the page.



Asset Info
Asset Discovered 89
Connections 9,204

Network Traffic Flow
Unicast 9,204
Multicast 0
Broadcast 0

Network Errors 16

Anomalies 608

Protocol Distribution

IT Protocols	86.4%
HTTPS	14042
HTTP	534
OT Protocols	0.1%
Telvent OASyS DNA	15
Siemens Spectrum Power TG	5
Other Protocols	13.4%
ARP	1635
Other	10

Errors & Anomalies

Security: HTTP 02 Apr 2024 @ 06:22:00 PM
52.26.57.248 → 10.20.254.130

Security: HTTP 02 Apr 2024 @ 06:21:59 PM
10.20.254.130 → 52.26.57.248

Security: HTTP 02 Apr 2024 @ 06:21:27 PM
34.209.222.202 → 10.20.254.130

Security: HTTP 02 Apr 2024 @ 06:21:27 PM
10.20.254.130 → 34.209.222.202

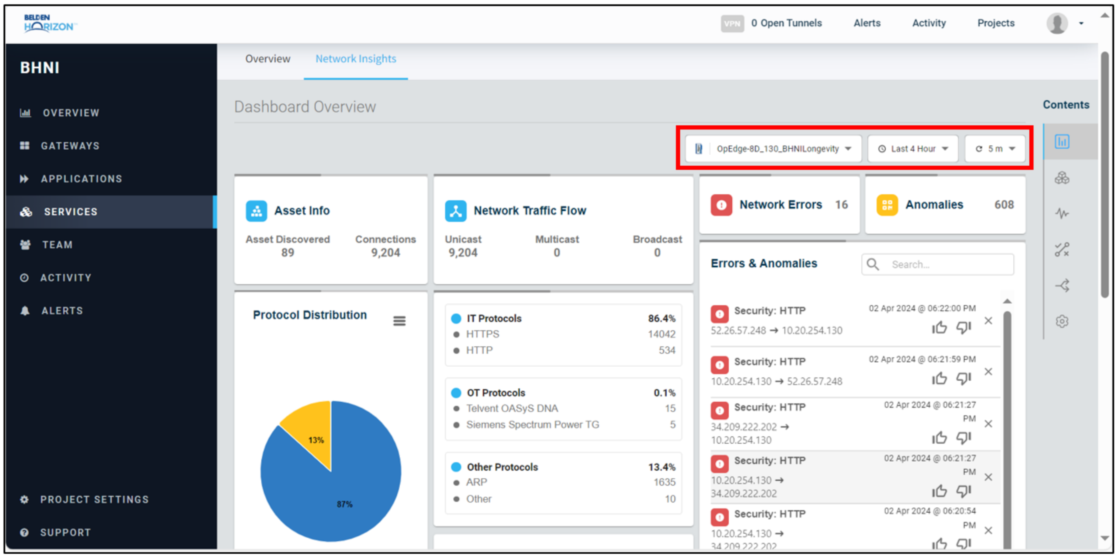
Security: HTTP 02 Apr 2024 @ 06:20:54 PM
10.20.254.130 → 34.209.222.202

The following Network Insights menus are available in the **Contents** panel:

- Dashboard Overview
- Assets Menu
- Performance Menu
- Alerts & Anomalies Menu
- Traffic Flow Menu
- Settings Menu

11 Three drop-down lists are present in each of the Network Insights menus:

- Select the device to view the Network insights.
- Select the time frame.
- Select the refresh duration of the dashboard.



Dashboard Overview

OpEdge-8D_130_BHNILongevity | Last 4 Hour | 5 m

Asset Info	
Asset Discovered	Connections
89	9,204

Network Traffic Flow		
Unicast	Multicast	Broadcast
9,204	0	0

Network Errors 16

Anomalies 608

Protocol Distribution

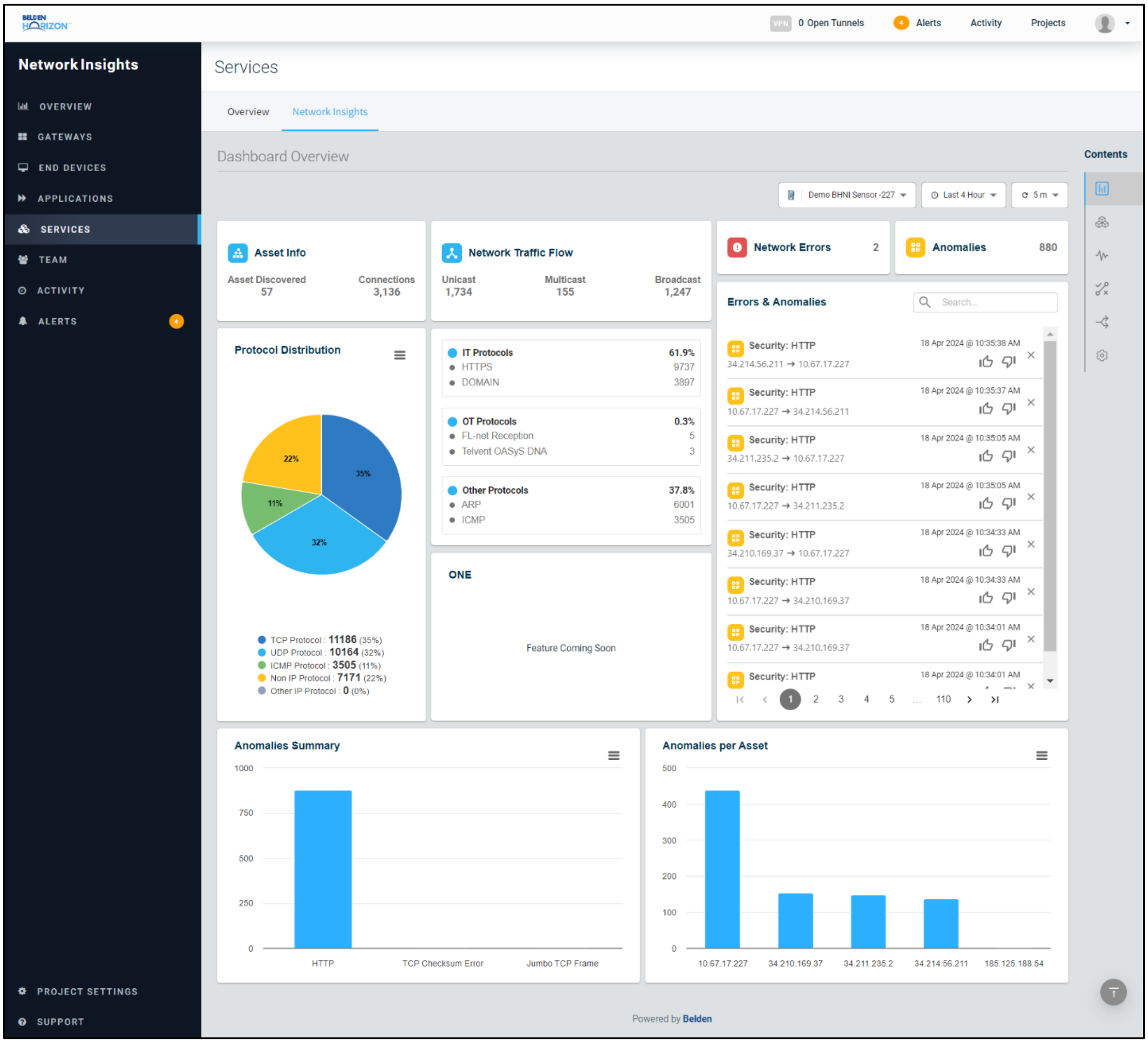
IT Protocols	86.4%
HTTPS	14042
HTTP	534
OT Protocols	0.1%
Telvent OASyS DNA	15
Siemens Spectrum Power TG	5
Other Protocols	13.4%
ARP	1635
Other	10

Errors & Anomalies

Security: HTTP 52.26.57.248 → 10.20.254.130	02 Apr 2024 @ 06:22:00 PM
Security: HTTP 10.20.254.130 → 52.26.57.248	02 Apr 2024 @ 06:21:59 PM
Security: HTTP 34.209.222.202 → 10.20.254.130	02 Apr 2024 @ 06:21:27 PM
Security: HTTP 10.20.254.130 → 34.209.222.202	02 Apr 2024 @ 06:21:27 PM
Security: HTTP 10.20.254.130 → 34.209.222.202	02 Apr 2024 @ 06:20:54 PM

4.1 Dashboard Overview

The *Dashboard Overview* contains various information about Network Insights.



Asset Info

Asset Discovered	Connections
57	3,136

Network Traffic Flow

Unicast	Multicast	Broadcast
1,734	155	1,247

Network Errors 2

Anomalies 880

IT Protocols	61.9%
HTTPS	9737
DOMAIN	3897
OT Protocols	0.3%
FL-net Reception	5
Telvent OASyS DNA	3
Other Protocols	37.8%
ARP	6001
ICMP	3505

- TCP Protocol : 11186 (35%)
- UDP Protocol : 10164 (32%)
- ICMP Protocol : 3505 (11%)
- Non IP Protocol : 7171 (22%)
- Other IP Protocol : 0 (0%)

Errors & Anomalies

Security: HTTP	34.214.56.211 → 10.67.17.227	18 Apr 2024 @ 10:35:38 AM
Security: HTTP	10.67.17.227 → 34.214.56.211	18 Apr 2024 @ 10:35:37 AM
Security: HTTP	34.211.235.2 → 10.67.17.227	18 Apr 2024 @ 10:35:05 AM
Security: HTTP	10.67.17.227 → 34.211.235.2	18 Apr 2024 @ 10:35:05 AM
Security: HTTP	34.210.169.37 → 10.67.17.227	18 Apr 2024 @ 10:34:33 AM
Security: HTTP	10.67.17.227 → 34.210.169.37	18 Apr 2024 @ 10:34:33 AM
Security: HTTP	10.67.17.227 → 34.210.169.37	18 Apr 2024 @ 10:34:01 AM
Security: HTTP		18 Apr 2024 @ 10:34:01 AM

1 2 3 4 5 ... 110

4.1.1 Asset Info

The *Asset Info* section contains information of discovered assets and connections. Clicking inside the section redirects to the Assets Menu.

Parameter	Description
Asset Discovered	This displays the count of the discovered unique assets within the selected duration on the dashboard.
Connections	This displays the count of the connections between assets with unique IP address that are communicating within the monitored network (monitor port example eth0) within the selected duration on the dashboard.

4.1.2 Network Traffic Flow

The *Network Traffic Flow* section contains Unicast, Multicast and Broadcast information. Clicking inside the frame redirects to the Traffic Flow Menu.

Parameter	Description
Unicast	This displays the count of individual messages sent from one sender to one receiver within the network.
Multicast	This displays the count of messages sent from one sender to a group of receivers within the network.
Broadcast	This displays the count of messages sent from one sender to all the receivers within the network.

4.1.3 Network Errors

This displays the errors count. Clicking inside the frame redirects to the Alerts & Anomalies Menu.

4.1.4 Anomalies

This displays the anomalies count. Clicking inside the frame redirects to the Alerts & Anomalies Menu.

4.1.5 Errors & Anomalies

Refer to Errors & Anomalies.

4.1.6 Protocol Distribution

This displays the protocol sessions as a percentage in a pie chart within the selected duration on the dashboard.

- TCP Sessions
- UDP Sessions
- ICMP Sessions
- Non-IP Sessions
- Other IP Sessions

4.1.7 Anomalies Summary

This displays the anomalies count in a bar chart.

4.1.8 Anomalies per Asset

This displays the anomalies count for each asset in a bar chart.

4.2 Assets Menu

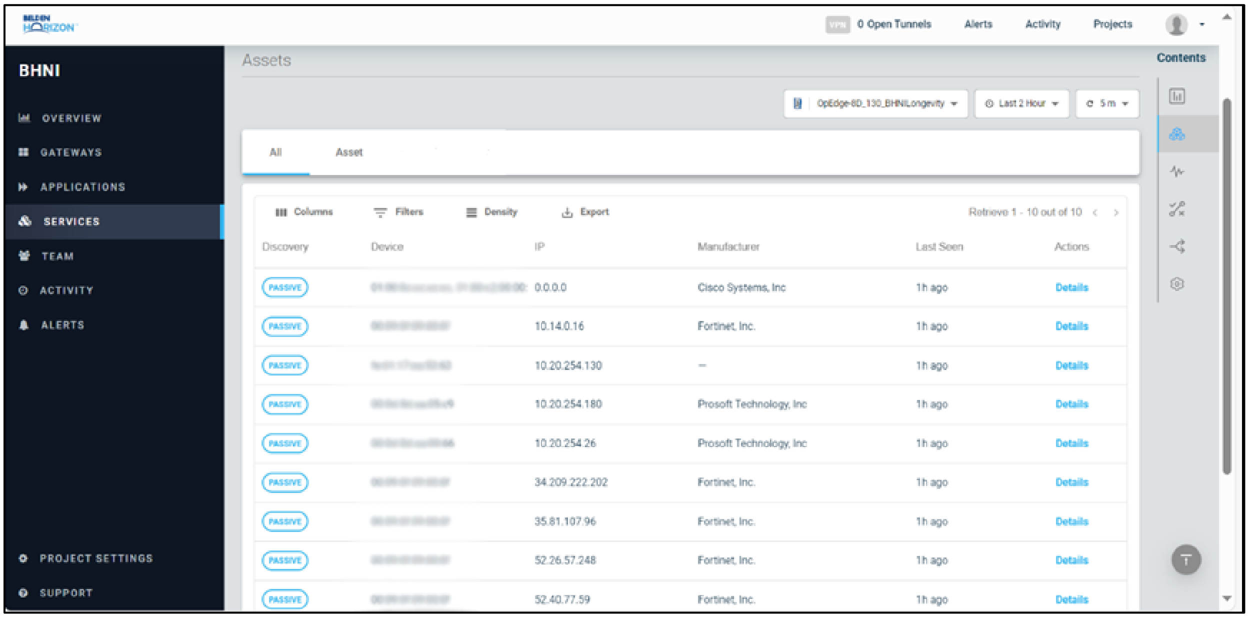
This menu consists of two tabs:

- *All*
- *Assets*

4.2.1 All Tab

The dashboard determines the details of a particular Asset found in the network within the selected duration. It provides the following information:

- Discovery (Active or Passive)
- Device MAC address
- IP address
- Manufacturer
- Last seen (time when the asset was last active in the network)



Assets

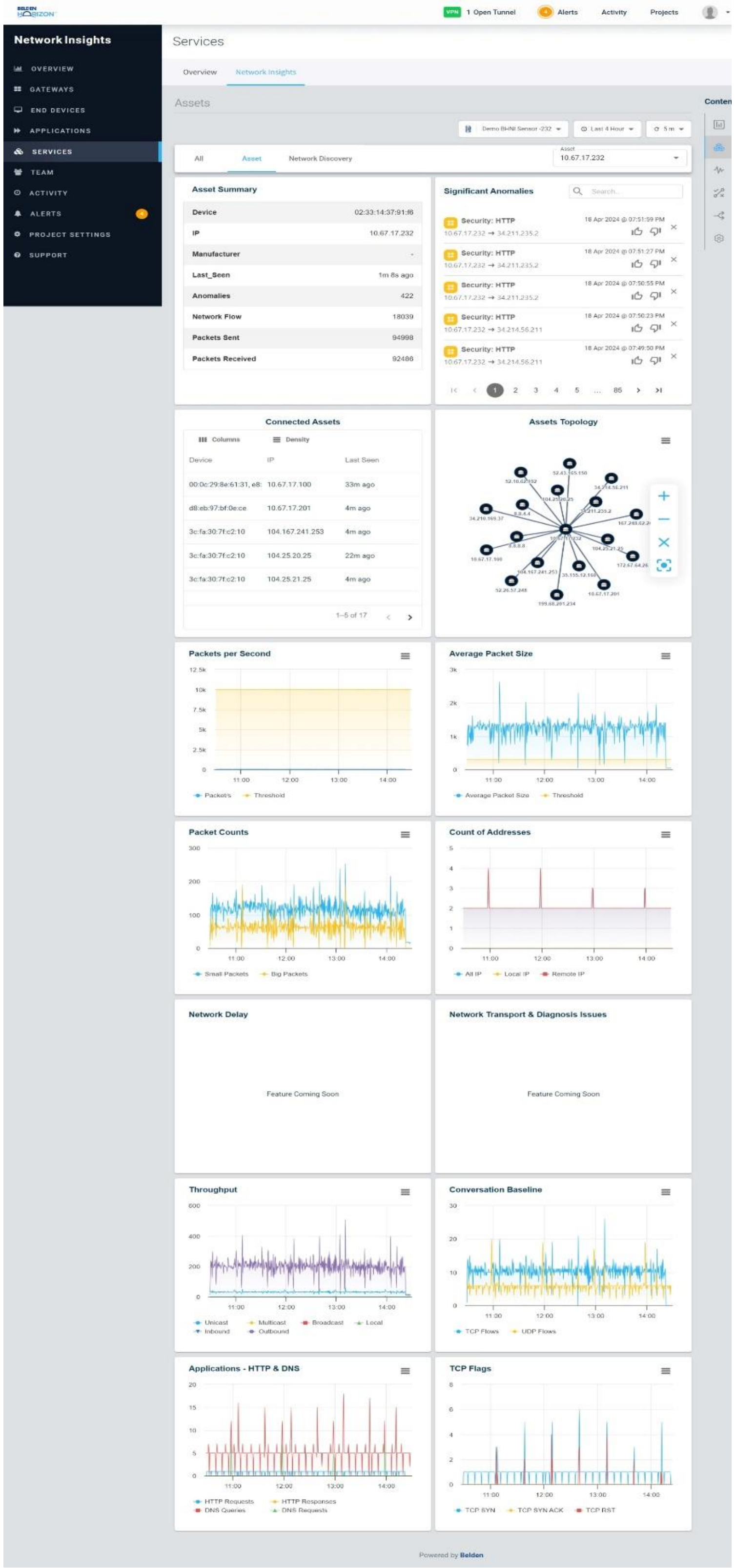
OpEdge-8D_130_BHNILongevity ▾ | Last 2 Hour ▾ | 5 m ▾

Retrieve 1 - 10 out of 10

Discovery	Device	IP	Manufacturer	Last Seen	Actions
PASSIVE	[redacted]	0.0.0.0	Cisco Systems, Inc	1h ago	Details
PASSIVE	[redacted]	10.14.0.16	Fortinet, Inc.	1h ago	Details
PASSIVE	[redacted]	10.20.254.130	–	1h ago	Details
PASSIVE	[redacted]	10.20.254.180	Prosoft Technology, Inc	1h ago	Details
PASSIVE	[redacted]	10.20.254.26	Prosoft Technology, Inc	1h ago	Details
PASSIVE	[redacted]	34.209.222.202	Fortinet, Inc.	1h ago	Details
PASSIVE	[redacted]	35.81.107.96	Fortinet, Inc.	1h ago	Details
PASSIVE	[redacted]	52.26.57.248	Fortinet, Inc.	1h ago	Details
PASSIVE	[redacted]	52.40.77.59	Fortinet, Inc.	1h ago	Details

4.2.2 Asset Tab

In the *Asset* tab, select the asset from the **ASSET** drop-down list to view its details. The following information is displayed:



Asset Summary

Device	02:33:14:37:91:f6
IP	10.67.17.232
Manufacturer	-
Last_Seen	1m 8s ago
Anomalies	422
Network Flow	18039
Packets Sent	94998
Packets Received	92486

Significant Anomalies

Security: HTTP 18 Apr 2024 @ 07:51:59 PM
10.67.17.232 → 34.211.235.2

Security: HTTP 18 Apr 2024 @ 07:51:27 PM
10.67.17.232 → 34.211.235.2

Security: HTTP 18 Apr 2024 @ 07:50:55 PM
10.67.17.232 → 34.211.235.2

Security: HTTP 18 Apr 2024 @ 07:50:23 PM
10.67.17.232 → 34.214.56.211

Security: HTTP 18 Apr 2024 @ 07:49:50 PM
10.67.17.232 → 34.214.56.211

1 2 3 4 5 ... 85

Connected Assets

Device	IP	Last Seen
00:0c:29:8e:61:31, e8:	10.67.17.100	33m ago
d8:eb:97:bf:0e:ce	10.67.17.201	4m ago
3c:fa:30:7f:c2:10	104.167.241.253	4m ago
3c:fa:30:7f:c2:10	104.25.20.25	22m ago
3c:fa:30:7f:c2:10	104.25.21.25	4m ago

1–5 of 17

Parameter	Description
Asset Summary	This displays the details of a particular Asset for the selected duration on the dashboard (example: last 4 hours, last 12 hours, etc.). It provides information such as: • Device (MAC Address) • IP address • Last seen time (time when the asset was last active on the network) • Anomalies (number of variations on the network involving this asset) • Network Flow (total number of packets transferred from the asset) • Packets Sent (number of packets sent by the asset) • Packets Received (number of packets received by the asset).
Significant Anomalies	This determines the details of anomalies present for a particular Asset with a specific source IP address found in the network within the selected duration on the dashboard (example: last 4 hours, last 12 hours, etc.) in seconds, which are not calculated by the Machine Learning.
Connected Assets	This displays the list of Assets that are connected to the asset selected by the user from the **Asset** drop-down list for the selected duration (example: last 4 hours, last 12 hours, etc.). It provides information such as: • MAC Address • IP address • Last seen time (time when the asset was last active on the network)
Assets Topology	This determines the source address, destination address, and the flow of packets for a particular asset found in the network within the selected duration on the dashboard (example: last 4 hours, last 12 hours, etc.) in seconds. This reveals how the assets are connected and how the data is flowing.
Packets per Second	This calculation determines the total number of packets sent divided by the selected duration on the dashboard (example: last 4 hours, last 12 hours, etc.) in seconds. The result represents the packets per second.
Average Packet Size	This displays the average length of the packets for a specific Asset with a particular source IP address found in the network within the selected duration on the dashboard (example: last 4 hours, last 12 hours, etc.) in seconds.
Packet Counts	This calculation determines the total number of small packets and big packets within the selected duration on the dashboard (example: last 4 hours, last 12 hours, etc.) in seconds.
Count of Addresses	This determines the count of IP addresses for a specific Asset with a particular source IP address found in the network within the selected duration on the dashboard (example: last 4 hours, last 12 hours, etc.) in seconds. These counts are calculated separately as *All IP*, *Local IP*, and *Remote IP*.
Throughput	This determines the number of packets transmitted for a specific Asset found in the network within the selected duration on the dashboard (example: last 4 hours, last 12 hours, etc.) in seconds. These calculations are done separately for Unicast, Multicast, Broadcast, Local, Inbound, and Outbound packets.
Conversation Baseline	This determines the count of packets for a specific Asset with a particular IP address found in the network within the selected duration on the dashboard (example: last 4 hours, last 12 hours, etc.) in seconds. These calculations are done separately for TCP flows and UDP flows.
Applications – HTTP & DNS	This process calculates the total number of HTTP requests and responses, DNS queries, and responses for a specific Asset with a particular IP address found in the network within the selected duration on the dashboard (example: last 4 hours, last 12 hours, etc.) in seconds. These calculations are performed separately for Unicast, Multicast, Broadcast, Local, Inbound, and Outbound packets.

TCP Flags	This process determines the TCP flag value (from the following parameters: SYN_FLAG_SET, SYN_ACK_FLAG_SET, RESET_FLAG_SET) for a specific Asset with a particular IP address found in the network within the selected duration on the dashboard (example: last 4 hours, last 12 hours, etc.) in seconds.

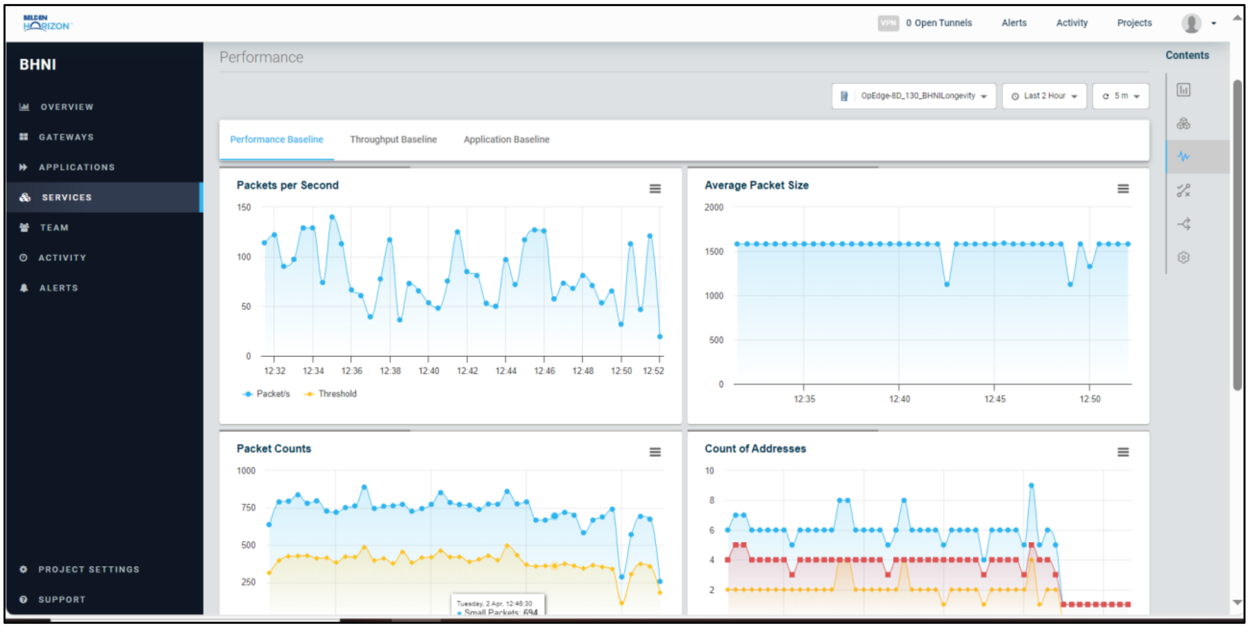
4.3 Performance Menu

This menu consists of three tabs:

- *Performance Baseline*
- *Throughput Baseline*
- *Application Baseline*

4.3.1 Performance Baseline

In the *Performance Baseline* tab, the following information is displayed:

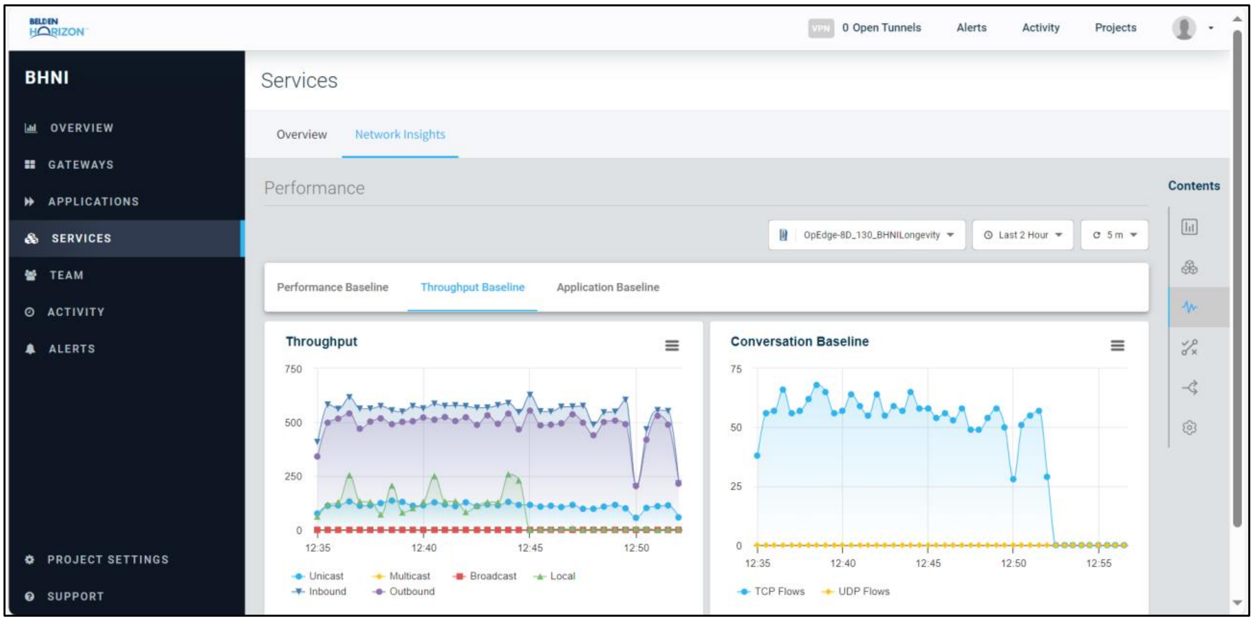


Parameter	Description
Packets per second	In the context of "Packet per Second" (PPS), performance refers to measuring how many individual data packets a network can process within one second. This metric is crucial for evaluating the efficiency and capacity of a network in handling data traffic. A higher PPS value indicates better performance, displaying the network's ability to manage a larger volume of packets and, consequently, support communication that is more concurrent.
Average Packet Size	The average packet size in a network affects performance. A smaller size can result in more frequent but smaller data transfers, while a larger size implies fewer but more significant transfers. This affects bandwidth usage, latency, and overall data throughput, underscoring the importance of optimizing packet sizes for efficient network operation.
Packet Counts	This in network performance refers to the tally of individual data packets transmitted or received. Monitoring these counts is crucial for evaluating network activity. A higher count may signal increased usage, potentially causing congestion. A lower count could indicate underutilization. Analyzing packet counts helps administrators identify trends, troubleshoot issues, and optimize network efficiency to achieve an optimal balance between capacity and usage for peak performance.

Counts of Addresses	This in network performance refers to the total number of unique addresses, such as IP addresses, in a network. It is a key metric for evaluating scalability and network management. Efficiently handling this count is vital to prevent conflicts and maintain smooth communication among devices.

4.3.2 Throughput Baseline

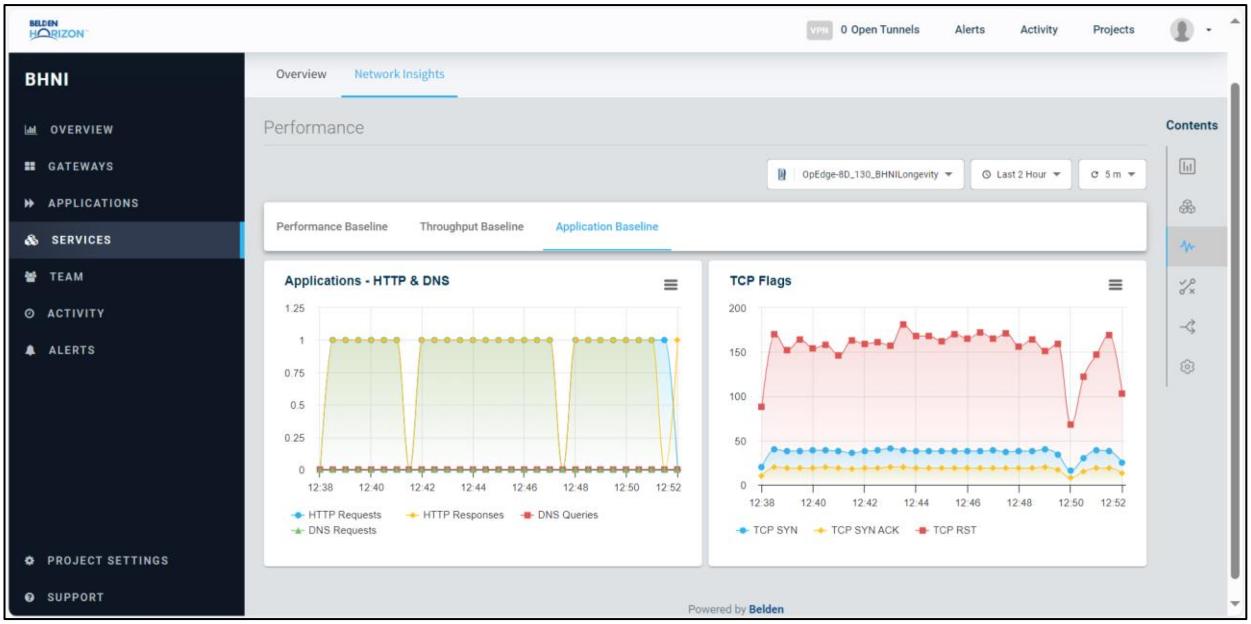
In the *Throughput Baseline* tab, the following information is displayed:



Parameter	Description
Throughput	Throughput, a key metric in network performance, quantifies the rate of successful data transmission. Unicast throughput evaluates the speed of point-to-point communication, multicast measures efficiency in one-to-many scenarios, and broadcast assesses one-to-all communication. Local throughput gauges data transfer within a specific network, while inbound and outbound throughputs quantify the speed of data received and sent externally. Optimizing these types of throughput is essential for enhancing network efficiency, reducing latency, and ensuring swift, reliable data transmission across diverse communication scenarios.
Conversation Baseline	Conversation Baseline visually represents communication patterns between devices in a network. By establishing a conversation baseline, network administrators can identify normal behavior, detect anomalies, and optimize performance. This approach aids in troubleshooting, security monitoring, and ensuring that network activities align with expected patterns for efficient and reliable operation.

4.3.3 Application Baseline

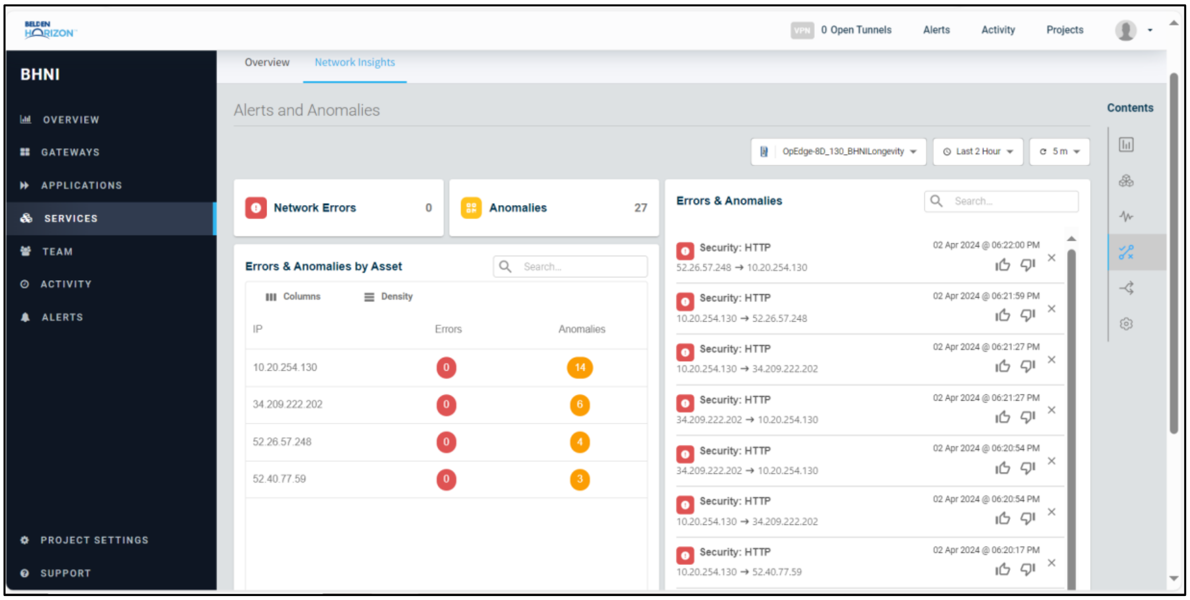
In the *Application Baseline* tab, the following information is displayed:



Parameter	Description
Applications HTTP & DNS	This process calculates the total number of HTTP requests and responses, DNS queries, and responses for a specific Asset with a particular IP address found in the network within the selected duration on the dashboard (example: last 4 hours, last 12 hours, etc.) in seconds.
TCP Flags	This process determines the TCP flag value (from the following parameters: SYN_FLAG_SET, SYN_ACK_FLAG_SET, RESET_FLAG_SET) for a specific Asset with a particular IP address found in the network within the selected duration on the dashboard (example: last 4 hours, last 12 hours, etc.) in seconds.

4.4 Alerts & Anomalies Menu

Networking Alerts are notifications or warnings generated by monitoring systems to inform administrators of specific events or conditions that may require attention. Anomalies refer to unexpected or abnormal patterns of behavior within the network that may indicate potential problems or security threats. Together, alerts and anomaly detection mechanisms contribute to the overall health and security of a network by providing real-time insights and facilitating prompt responses to emerging issues.



Alerts and Anomalies

OpEdge-8D_130_BHNILongevity | Last 2 Hour | 5 m

Network Errors 0

Anomalies 27

Errors & Anomalies by Asset

IP	Errors	Anomalies
10.20.254.130	0	14
34.209.222.202	0	6
52.26.57.248	0	4
52.40.77.59	0	3

Errors & Anomalies

Security: HTTP
52.26.57.248 → 10.20.254.130
02 Apr 2024 @ 06:22:00 PM

Security: HTTP
10.20.254.130 → 52.26.57.248
02 Apr 2024 @ 06:21:59 PM

Security: HTTP
10.20.254.130 → 34.209.222.202
02 Apr 2024 @ 06:21:27 PM

Security: HTTP
34.209.222.202 → 10.20.254.130
02 Apr 2024 @ 06:21:27 PM

Security: HTTP
34.209.222.202 → 10.20.254.130
02 Apr 2024 @ 06:20:54 PM

Security: HTTP
10.20.254.130 → 34.209.222.202
02 Apr 2024 @ 06:20:54 PM

Security: HTTP
10.20.254.130 → 52.40.77.59
02 Apr 2024 @ 06:20:17 PM

4.4.1 Network Errors

Network errors disrupt or cause problems that affect communication and data exchange between devices connected to the internet. These errors can result from issues such as server outages, DNS (Domain Name System) errors, bandwidth limitations, or problems with routers and switches. When network errors occur, users may experience slow internet speeds, website unavailability, or difficulty accessing online services. Timely troubleshooting and addressing issues are essential for maintaining a stable and reliable internet connection.

4.4.2 Anomalies

Anomalies refer to irregularities or deviations from the expected behavior within a computer network. These anomalies can encompass a wide range of events and behaviors, including unusual patterns of network traffic, unexpected changes in data transfer rates or abnormal activities that may indicate security threats.

4.4.3 Errors & Anomalies

Errors and anomalies disrupt or cause irregularities that can impacts the functionality, performance, and security of a computer network.

4.4.4 Errors & Anomalies by Asset

Monitoring errors and anomalies by asset involves tracking deviations or irregularities at the individual device or application level within a network. This approach provides detailed insights into the performance, security, and overall health of each asset. By identifying specific errors or anomalies associated with a particular asset, network administrators can efficiently troubleshoot, diagnose, and resolve issues, optimizing the overall reliability and security of the network.

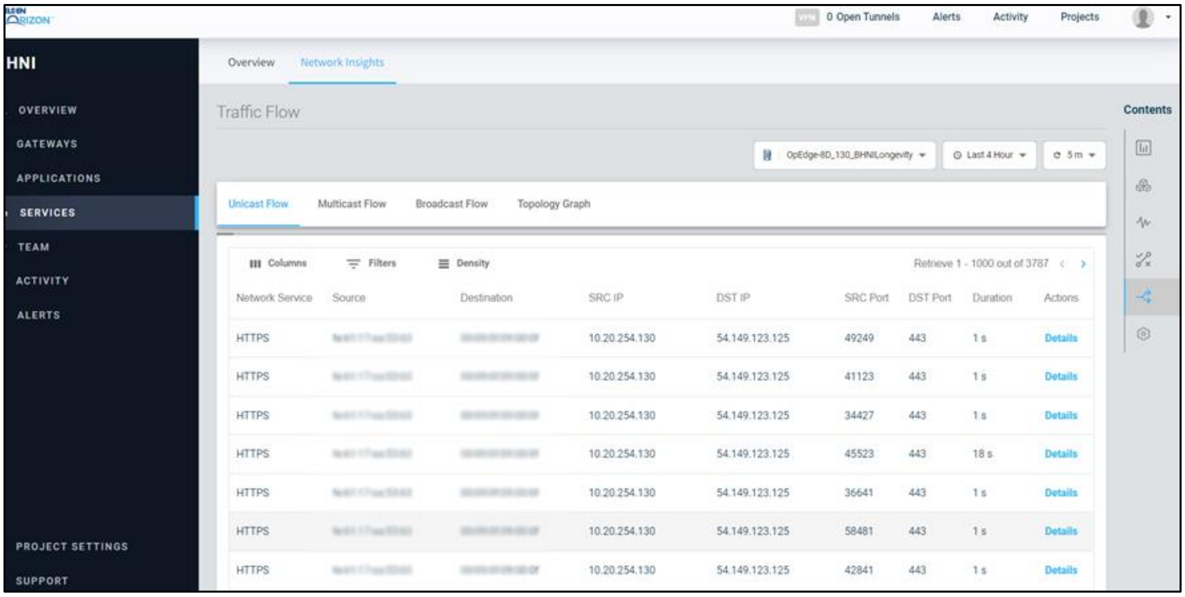
4.5 Traffic Flow Menu

This menu consists of four tabs:

- *Unicast Flow*
- *Multicast Flow*
- *Broadcast Flow*
- *Topology Graph*

4.5.1 Unicast Flow

Unicast refers to one-to-one communication, where data packets are sent from a single source to a single destination. For example, sending an email or loading a web page.

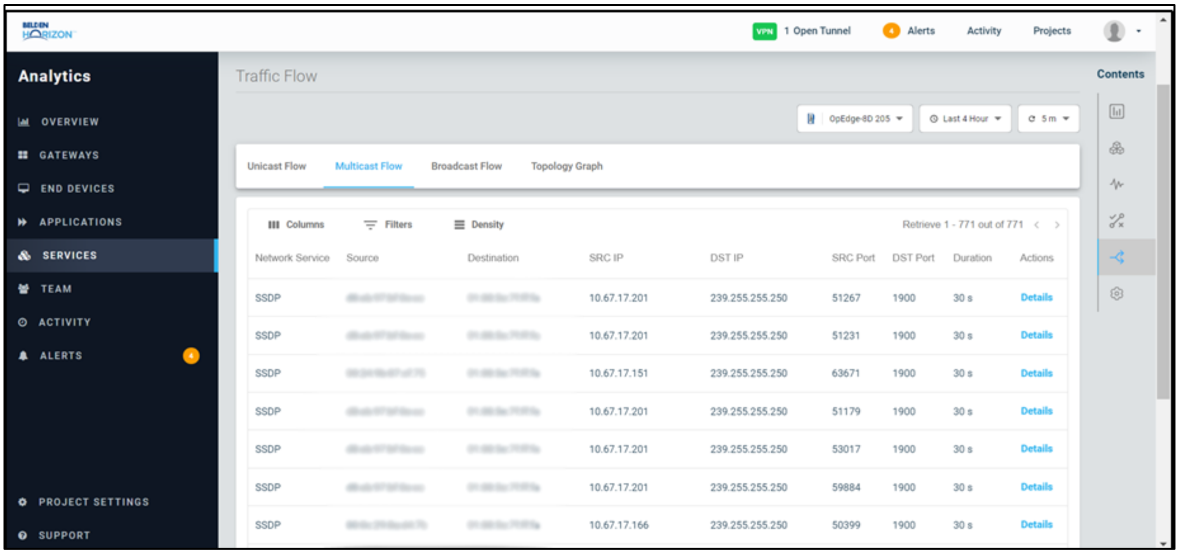


Retrieve 1 - 1000 out of 3787

Network Service	Source	Destination	SRC IP	DST IP	SRC Port	DST Port	Duration	Actions
HTTPS	[redacted]	[redacted]	10.20.254.130	54.149.123.125	49249	443	1 s	Details
HTTPS	[redacted]	[redacted]	10.20.254.130	54.149.123.125	41123	443	1 s	Details
HTTPS	[redacted]	[redacted]	10.20.254.130	54.149.123.125	34427	443	1 s	Details
HTTPS	[redacted]	[redacted]	10.20.254.130	54.149.123.125	45523	443	18 s	Details
HTTPS	[redacted]	[redacted]	10.20.254.130	54.149.123.125	36641	443	1 s	Details
HTTPS	[redacted]	[redacted]	10.20.254.130	54.149.123.125	58481	443	1 s	Details
HTTPS	[redacted]	[redacted]	10.20.254.130	54.149.123.125	42841	443	1 s	Details

4.5.2 Multicast Flow

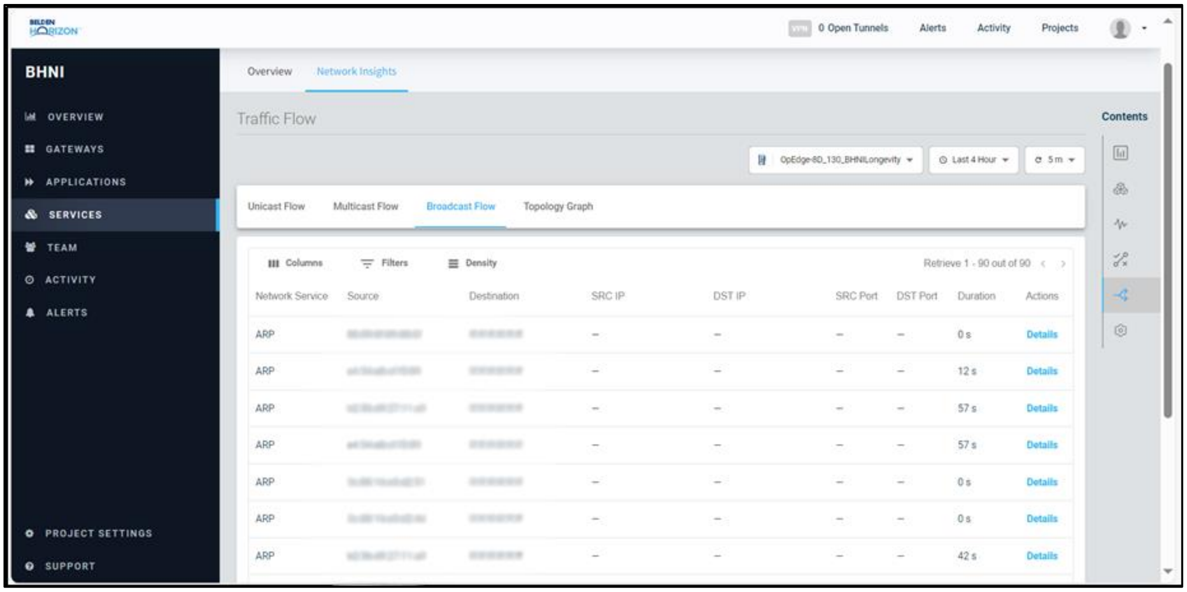
Multicast refers to one-to-many or many-to-many communication, in which data packets are sent from one source to multiple specific destinations. For example, streaming video to multiple recipients simultaneously.



Network Service	Source	Destination	SRC IP	DST IP	SRC Port	DST Port	Duration	Actions
SSDP	[redacted]	[redacted]	10.67.17.201	239.255.255.250	51267	1900	30 s	Details
SSDP	[redacted]	[redacted]	10.67.17.201	239.255.255.250	51231	1900	30 s	Details
SSDP	[redacted]	[redacted]	10.67.17.151	239.255.255.250	63671	1900	30 s	Details
SSDP	[redacted]	[redacted]	10.67.17.201	239.255.255.250	51179	1900	30 s	Details
SSDP	[redacted]	[redacted]	10.67.17.201	239.255.255.250	53017	1900	30 s	Details
SSDP	[redacted]	[redacted]	10.67.17.201	239.255.255.250	59884	1900	30 s	Details
SSDP	[redacted]	[redacted]	10.67.17.166	239.255.255.250	50399	1900	30 s	Details

4.5.3 Broadcast Flow

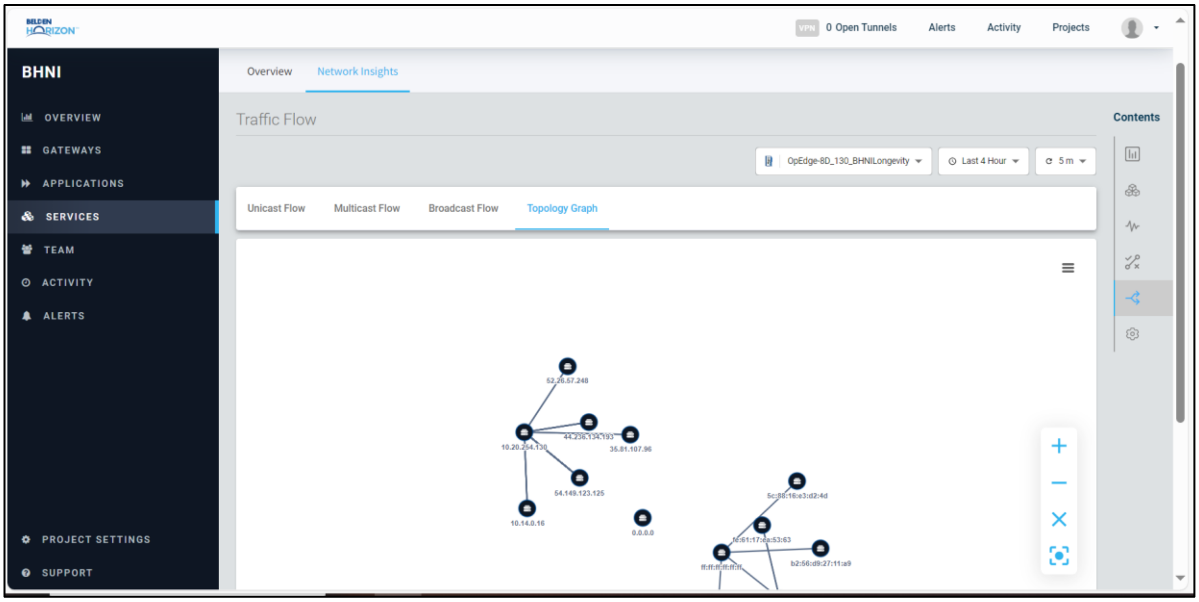
Broadcasting refers to one-to-all communication, where data packets are sent from a single source to all devices within the network. For example, broadcasting a message to all devices on a local network.



Network Service	Source	Destination	SRC IP	DST IP	SRC Port	DST Port	Duration	Actions
ARP	[redacted]	[redacted]	–	–	–	–	0 s	Details
ARP	[redacted]	[redacted]	–	–	–	–	12 s	Details
ARP	[redacted]	[redacted]	–	–	–	–	57 s	Details
ARP	[redacted]	[redacted]	–	–	–	–	57 s	Details
ARP	[redacted]	[redacted]	–	–	–	–	0 s	Details
ARP	[redacted]	[redacted]	–	–	–	–	0 s	Details
ARP	[redacted]	[redacted]	–	–	–	–	42 s	Details

4.5.4 Topology Graph

The Topology Graph is a visual representation that illustrates the arrangement of interconnected devices in a computer network and the paths along which data flows between them. It highlights the relationships and connections among network components.



4.6 Settings Menu

This menu consists of three tabs:

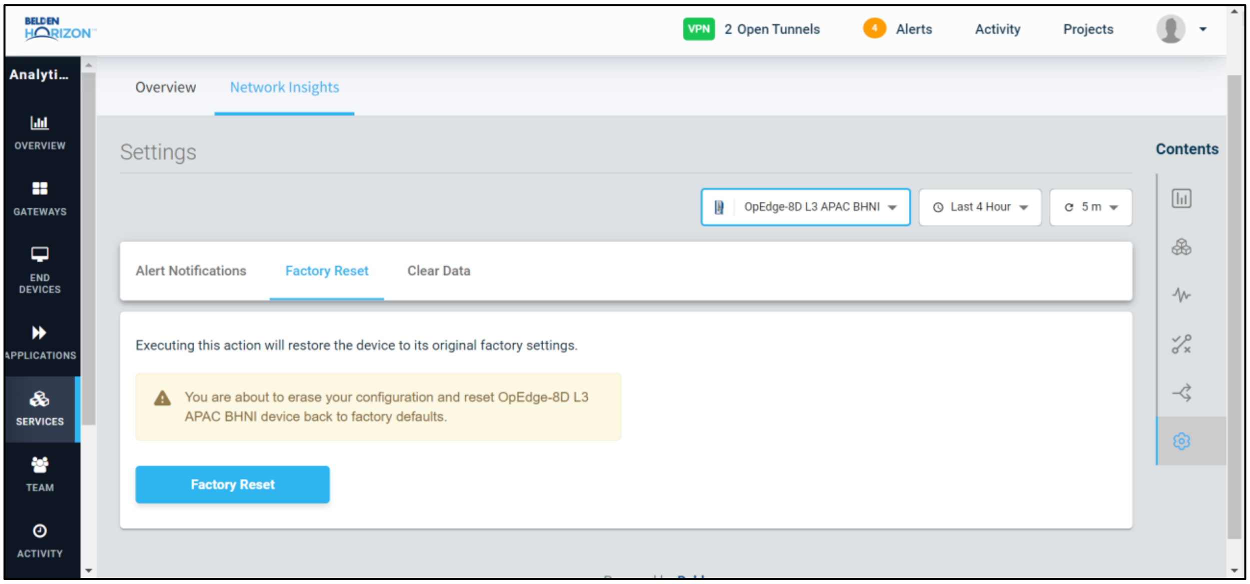
- *Alert Notifications*
- *Factory Reset*
- *Clear Data*

4.6.1 Alert Notifications

Feature coming soon.

4.6.2 Factory Reset

The *Factory Reset* tab can be used to reset the device to its factory settings. To do this, click the **FACTORY RESET** button and confirm.

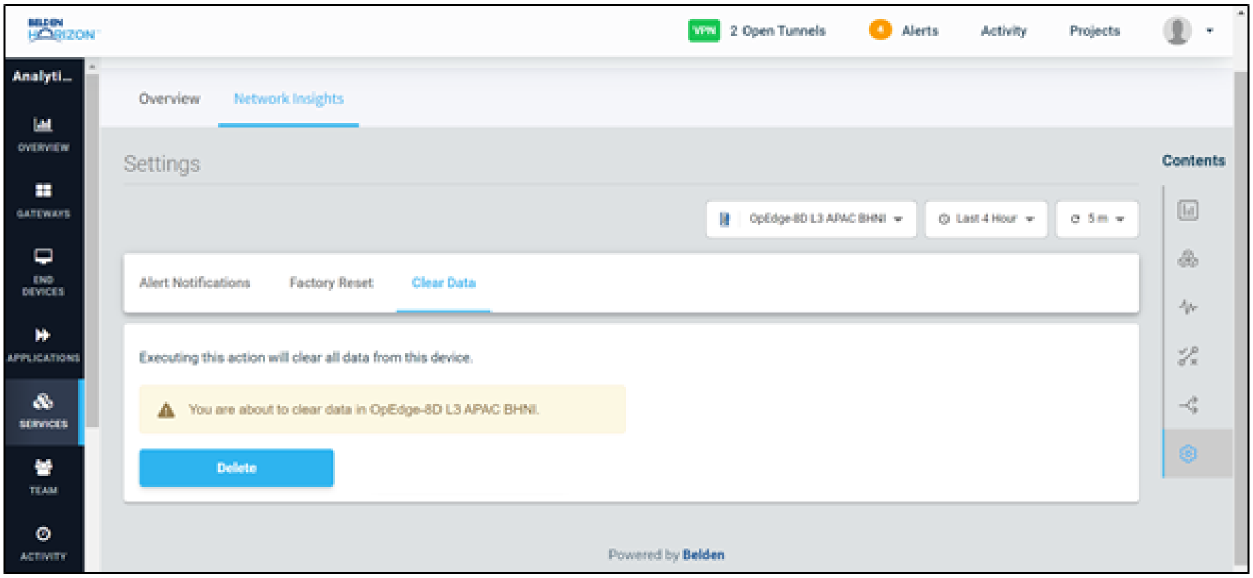


Executing this action will restore the device to its original factory settings.

You are about to erase your configuration and reset OpEdge-8D L3 APAC BHNI device back to factory defaults.

4.6.3 Clear Data

The *Clear Data* tab can be used to clear the data for the device. To do this, click the **DELETE** button.



Executing this action will clear all data from this device.

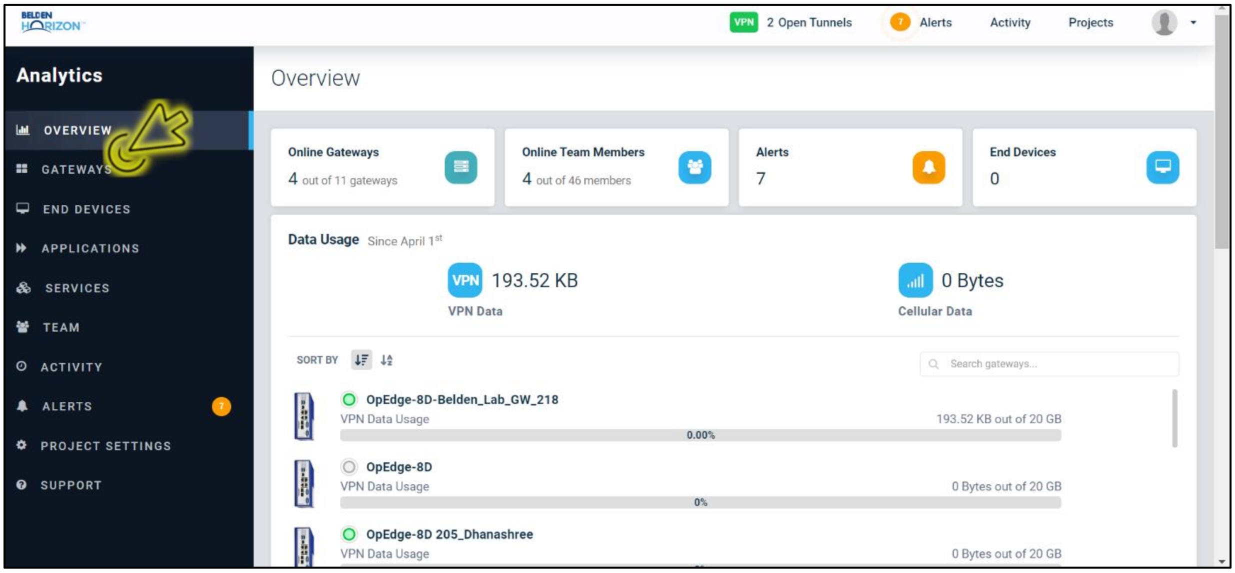
You are about to clear data in OpEdge-8D L3 APAC BHNI.

5 Container Removal

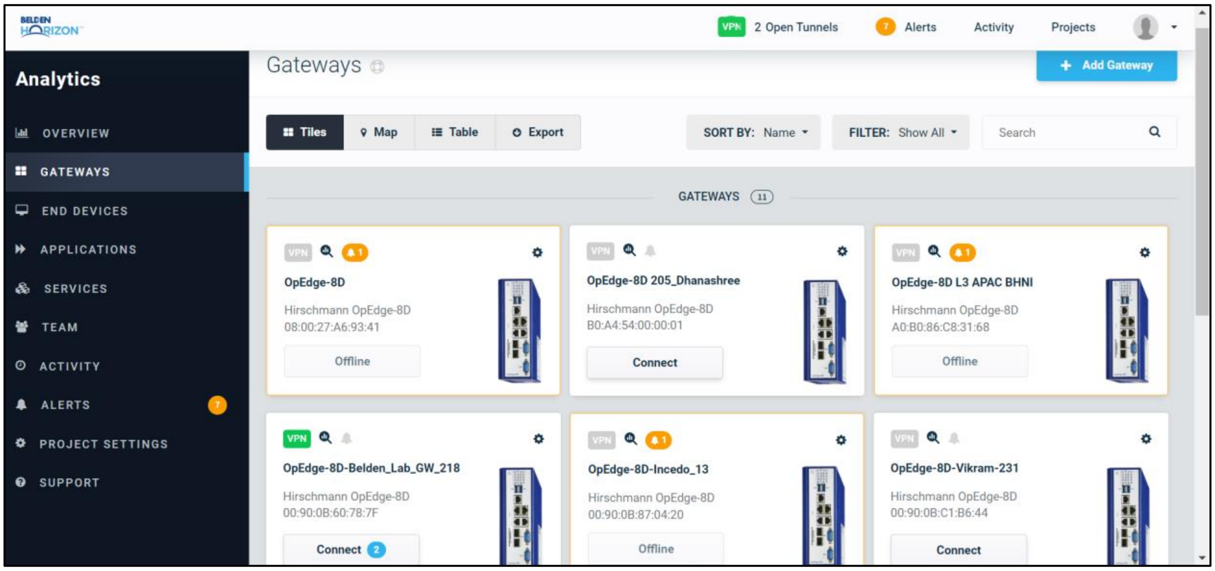
To remove an installed container, perform following steps:

1 Open the website https://belden.io and log in.

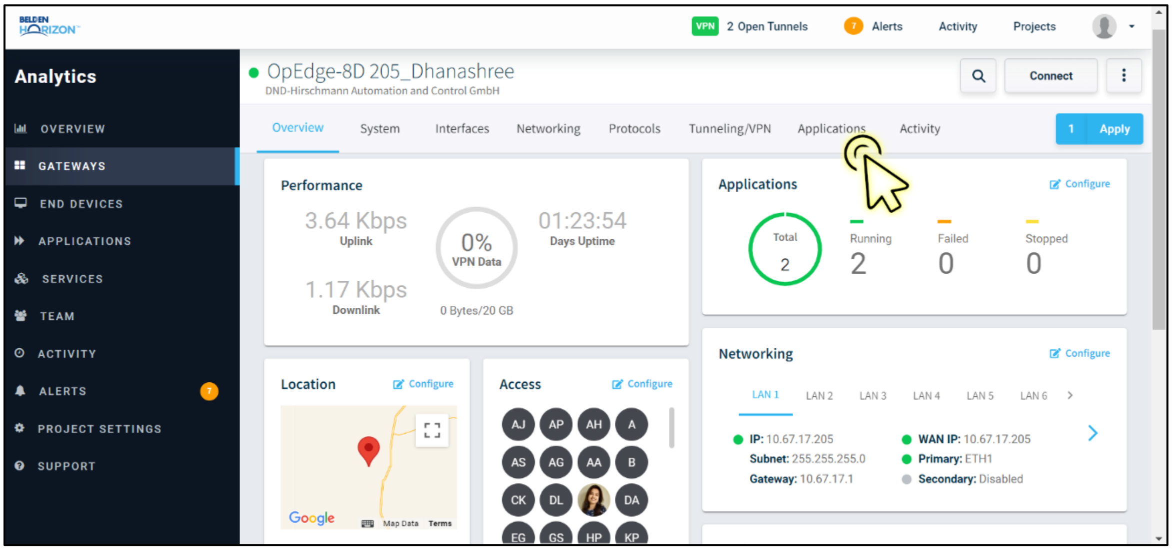
2 Click on **GATEWAYS** in the left panel.



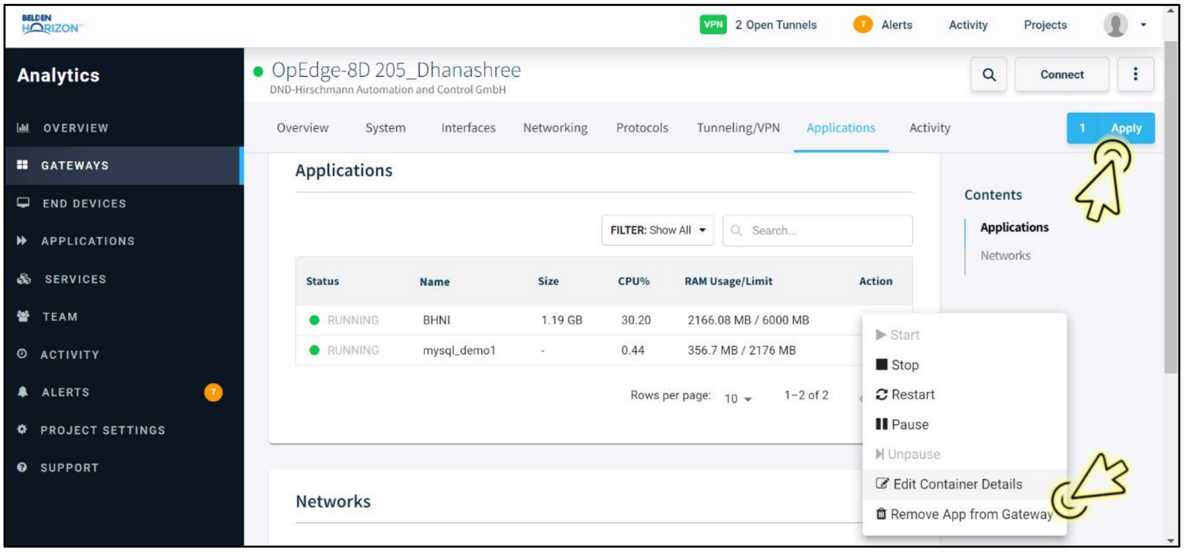
3 Click on the relevant gateway name to open its *Overview* page.



4 Click on the *Applications* tab.



5 Locate the relevant container and select the **REMOVE APP FROM GATEWAY** option in the *Action* column. This will remove the container from the gateway. Then click on the **APPLY** button.



Status	Name	Size	CPU%	RAM Usage/Limit	Action
● RUNNING	BHNI	1.19 GB	30.20	2166.08 MB / 6000 MB	
● RUNNING	mysql_demo1	-	0.44	356.7 MB / 2176 MB	

6 Support, Service, and Warranty

6.1 Contacting Technical Support

ProSoft Technology, Inc. is committed to providing the most efficient and effective support possible. Before calling, please gather the following information to assist in expediting this process:

1. Product Version Number
2. System architecture
3. Network details

If the issue is hardware related, we will also need information regarding:

1. Module configuration and associated ladder files, if any
2. Module operation and any unusual behavior
3. Configuration/Debug status information
4. LED patterns
5. Details about the interfaced serial, Ethernet or Fieldbus devices

Note: For technical support calls within the United States, ProSoft Technology's 24/7 after-hours phone support is available for urgent plant-down issues.

North America (Corporate Location)	Europe / Middle East / Africa Regional Office
Phone: +1.661.716.5100 info@prosoft-technology.com Languages spoken: English, Spanish REGIONAL TECH SUPPORT support@prosoft-technology.com	Phone: +33.(0)5.34.36.87.20 france@prosoft-technology.com Languages spoken: French, English REGIONAL TECH SUPPORT support.emea@prosoft-technology.com
Latin America Regional Office	**Asia Pacific Regional Office**
Phone: +52.222.264.1814 latinam@prosoft-technology.com Languages spoken: Spanish, English REGIONAL TECH SUPPORT support.la@prosoft-technology.com	Phone: +60.3.2247.1898 asiapc@prosoft-technology.com Languages spoken: Bahasa, Chinese, English, Japanese, Korean REGIONAL TECH SUPPORT support.ap@prosoft-technology.com

For additional ProSoft Technology contacts in your area, please visit: www.prosoft-technology.com/About-Us/Contact-Us.

6.2 Warranty Information

For complete details regarding ProSoft Technology's TERMS & CONDITIONS OF SALE, WARRANTY, SUPPORT, SERVICE AND RETURN MATERIAL AUTHORIZATION INSTRUCTIONS, please see the documents at: www.prosoft-technology/legal