



# Threat Prevention

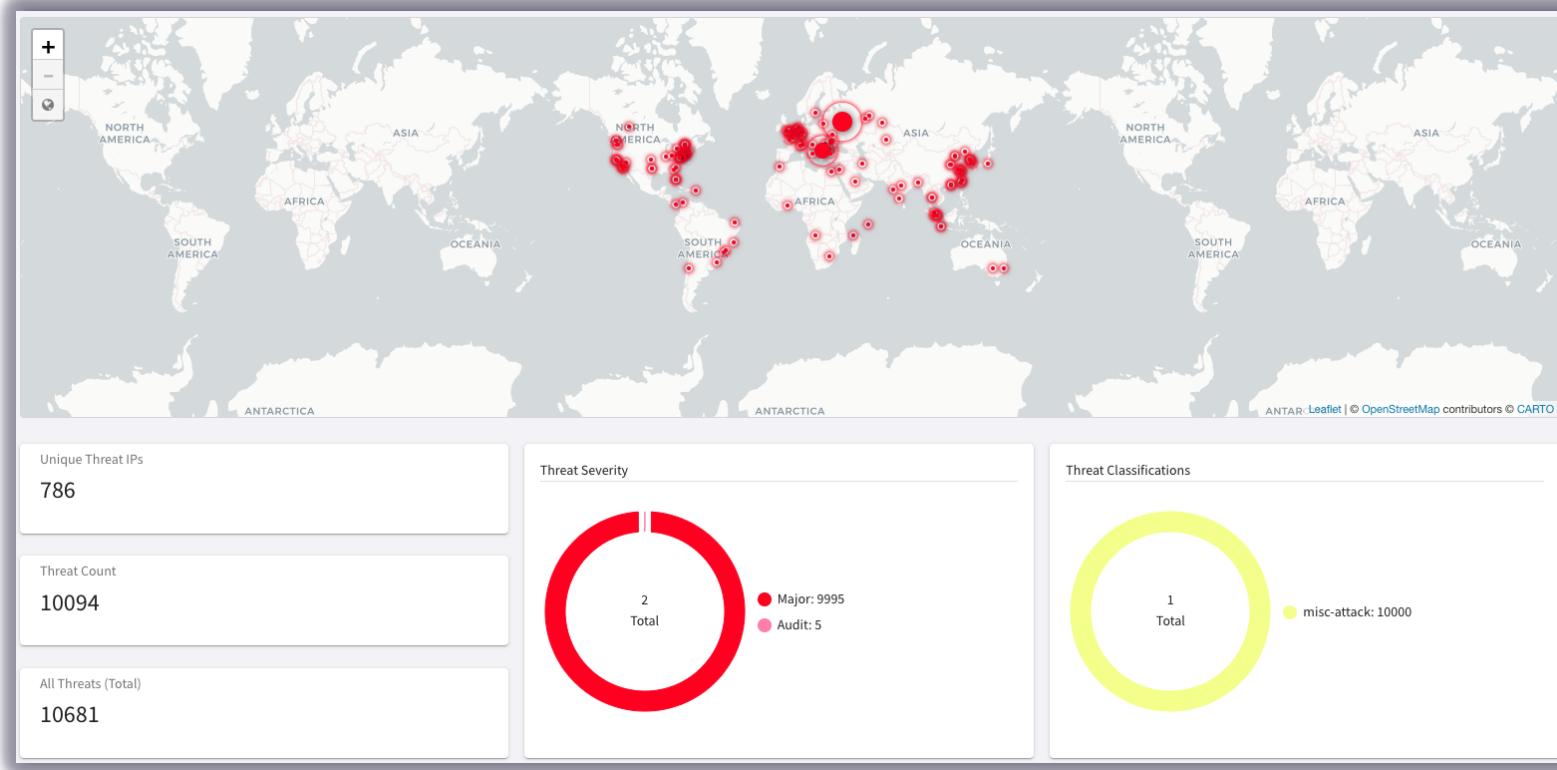
IDENTIFY AND REMEDIATE THREATS ACROSS MULTICLOUD NETWORKS

ACE Team



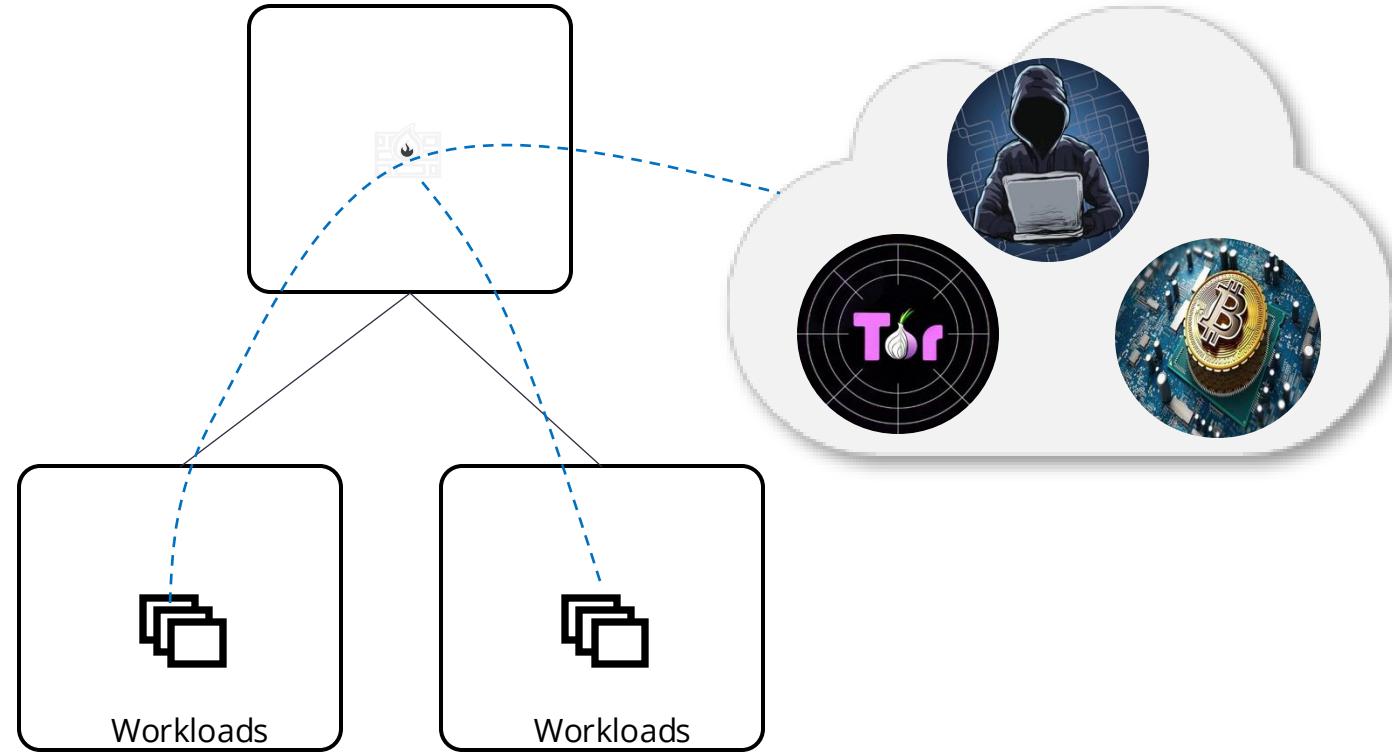
# What is it?

- Multicloud native network security to dynamically **identify, alert, and remediate potential threats** to known malicious IP addresses
- **Distributed threat visibility** and control built into the Distributed Cloud Firewall service using the *ThreatGroup*
- Identify potential **data exfiltration and compromised host**
- **Complementary security solution** with full multicloud support



# Why should enterprises care about threats?

- Internet access is everywhere in the cloud and on by default for some CSPs
- Funneling traffic through choke points or 3rd party services is inefficient and ineffective
- Protect business from security risks associated with:
  - Data exfiltration
  - Botnets
  - Compromised hosts
  - Crypto mining
  - TOR
  - DDoS, and more



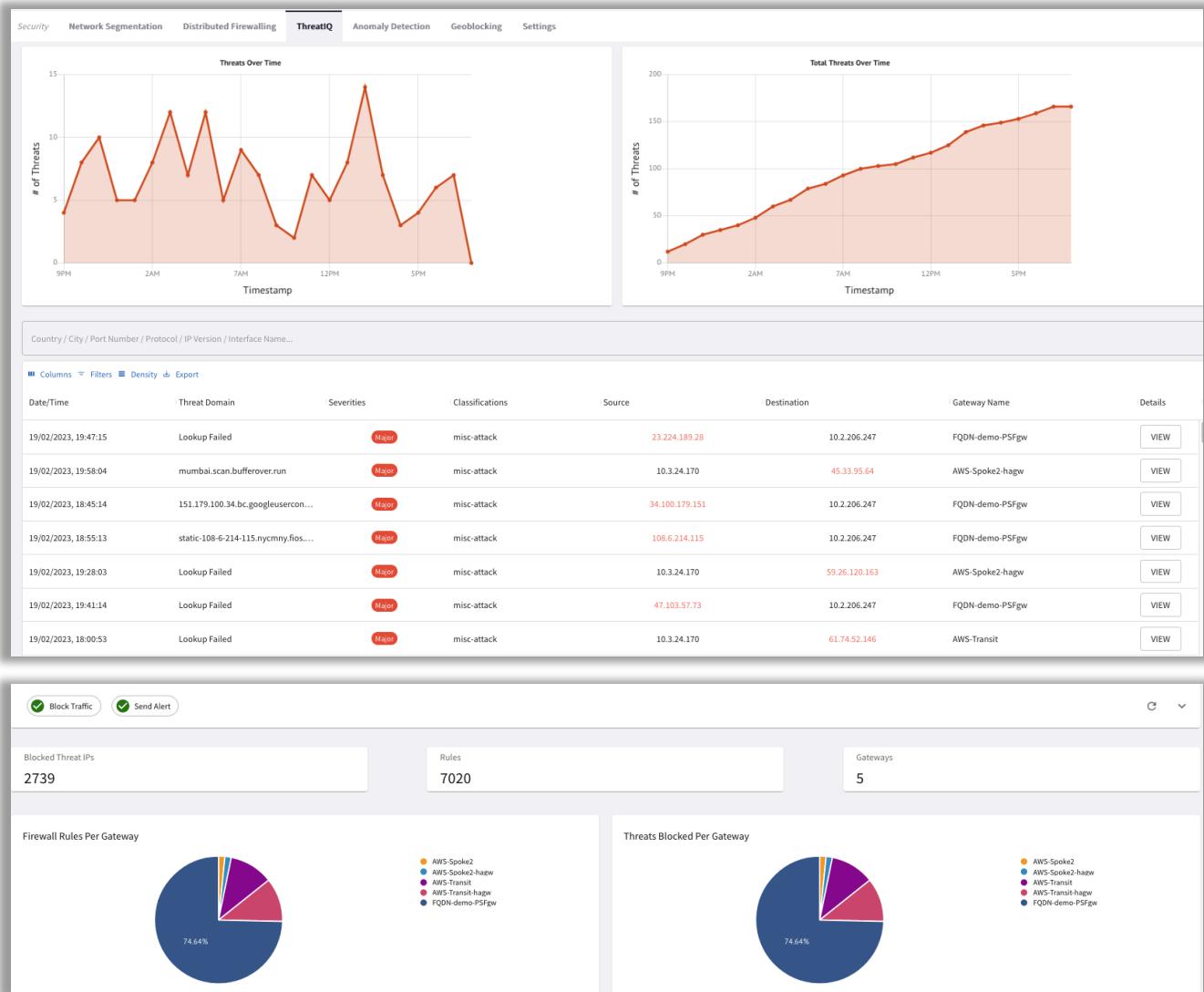
# How does it work?

## ● Distributed Inspection & Notification

- Aviatrix gateways across Multicloud environment send real-time NetFlow data to CoPilot
- CoPilot analyzes the data on all public destinations against well-known Threat DB.
- CoPilot alerts on any potential threats in the environment
- CoPilot provides extreme visibility of the impacted communication flow

## ● Distributed Enforcement

- CoPilot informs Aviatrix Controller to push firewall policies to all the Aviatrix gateways in the data path
- Firewall policies automatically get updated with the current status of the threat.
- Blocking threats with firewall policy is optional but recommended



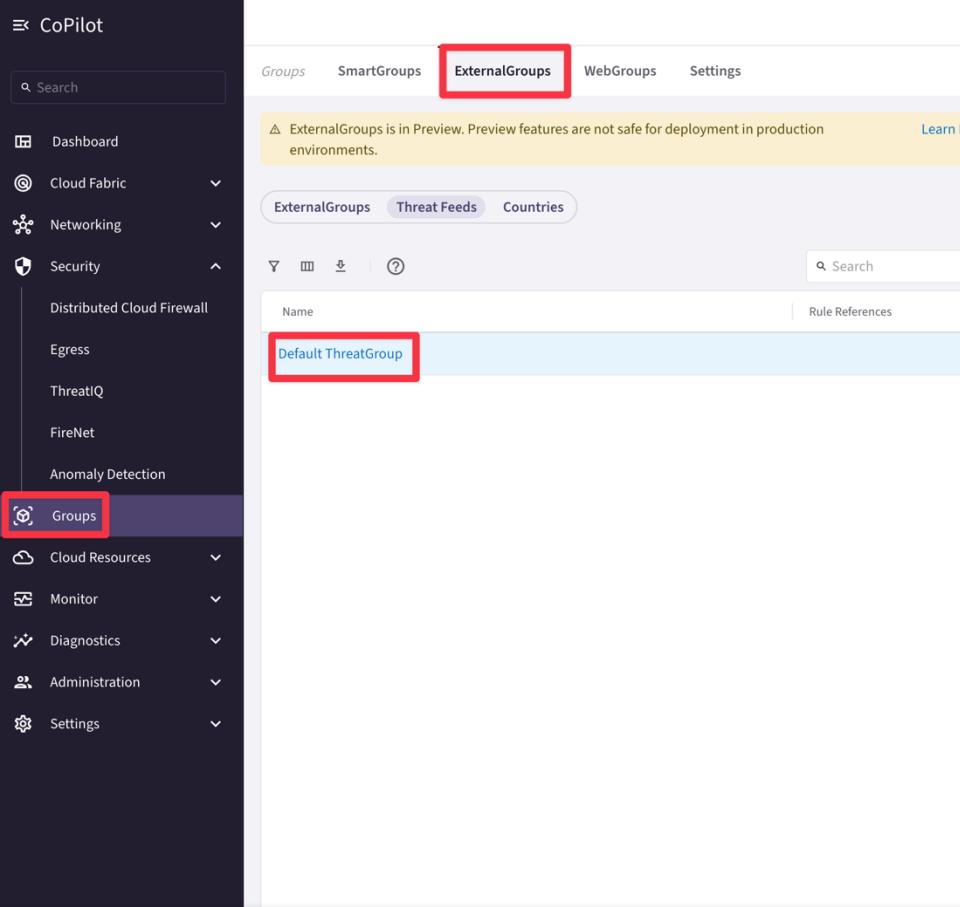
# Default ThreatGroup

## ● ProofPoint Database

- The **Default ThreatGroup** can be used to ensure that traffic meeting the ThreatGroup criteria is blocked
- The **Default ThreatGroup** is regularly updated with data from *ProofPoint Global Threat Defense Database* (every 30 min)
- The Default ThreatGroup references the complete list of all the Malicious IP addresses.

## ➤ Note:

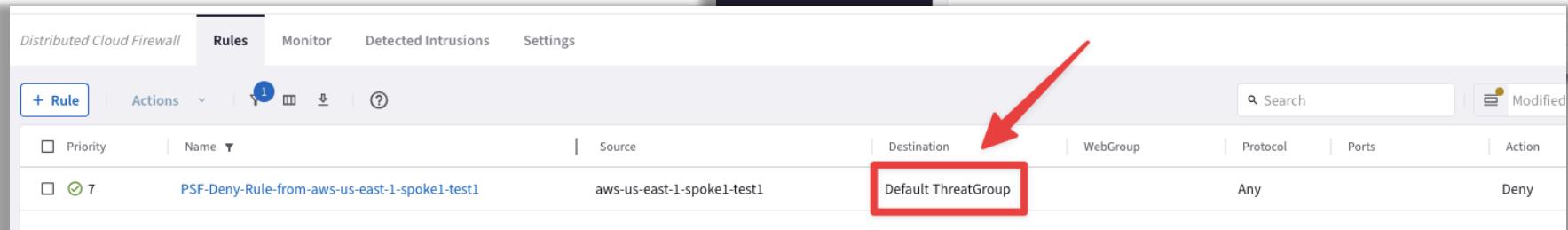
- You cannot have a ThreatGroup as both source and a destination in a DCF rule



ExternalGroups is in Preview. Preview features are not safe for deployment in production environments.

IP Address / CIDRs	Protocol	Threat Type	Severity
1.2.202.167/32		Threat Feed	Unknown
1.6.53.205/32		Threat Feed	Unknown
1.12.245.182/32		Threat Feed	Unknown
1.12.246.6/32		Threat Feed	Unknown
1.14.193.147/32		Threat Feed	Unknown
1.24.16.5/32		Threat Feed	Unknown
1.24.16.6/32		Threat Feed	Unknown
1.24.16.19/32		Threat Feed	Unknown
1.24.16.25/32		Threat Feed	Unknown
1.24.16.32/32		Threat Feed	Unknown
1.24.16.68/32		Threat Feed	Unknown
1.24.16.80/32		Threat Feed	Unknown
1.24.16.86/32		Threat Feed	Unknown
1.24.16.87/32		Threat Feed	Unknown

Total 11,707 IP Addresses



# ThreatIQ

## ● Overview Tab

- Shows a geographical map with the approximate locations of known malicious IPs that have communicated with your network within the specified time period selected.
- You can view the severity level of detected threat IPs and their associated attack classifications (as categorized by the well-known threat IPs DB).

The screenshot displays the ThreatIQ CoPilot interface with the 'Overview' tab selected. The left sidebar contains a navigation menu with options like Dashboard, Cloud Fabric, Networking, Security, ThreatIQ, FireNet, Anomaly Detection, Groups, Cloud Resources, Monitor, Diagnostics, Administration, and Settings. The main area features a world map showing the approximate locations of known malicious IPs. Below the map are three circular dashboards: 'Unique Threat IPs' (55), 'Threat Severity' (Total 55), and 'Threat Classifications' (Total 55). At the bottom, there are two line charts: 'Threats Over Time' (showing a sharp increase around 6:00 PM) and 'Total Threats Over Time' (showing a steady increase over the day). A table at the bottom lists threat details with columns for Timestamp, Threat Domain, Severities, Classifications, Source, Destination, and Gateway Name, along with a 'VIEW' link for each row.

Timestamp	Threat Domain	Severities	Classifications	Source	Destination	Gateway Name	Actions
Dec 18, 2024 9:15:25 PM	Lookup Failed	● Major	misc-attack	4.228.225.246	10.0.12.40	aws-us-east-1-psf	<a href="#">VIEW</a>
Dec 18, 2024 9:09:38 PM	andreas.probe.onyphe.net	● Major	misc-attack	51.81.110.52	10.0.12.40	aws-us-east-1-psf	<a href="#">VIEW</a>
Dec 18, 2024 9:08:02 PM	33.211.203.35.bc.googleus...	● Major	misc-attack	35.203.211.33	10.0.12.40	aws-us-east-1-psf	<a href="#">VIEW</a>
Dec 18, 2024 9:08:02 PM	warsaw.scan.bufferover.run	● Major	misc-attack	45.79.132.41	10.0.12.40	aws-us-east-1-psf	<a href="#">VIEW</a>



# CostIQ

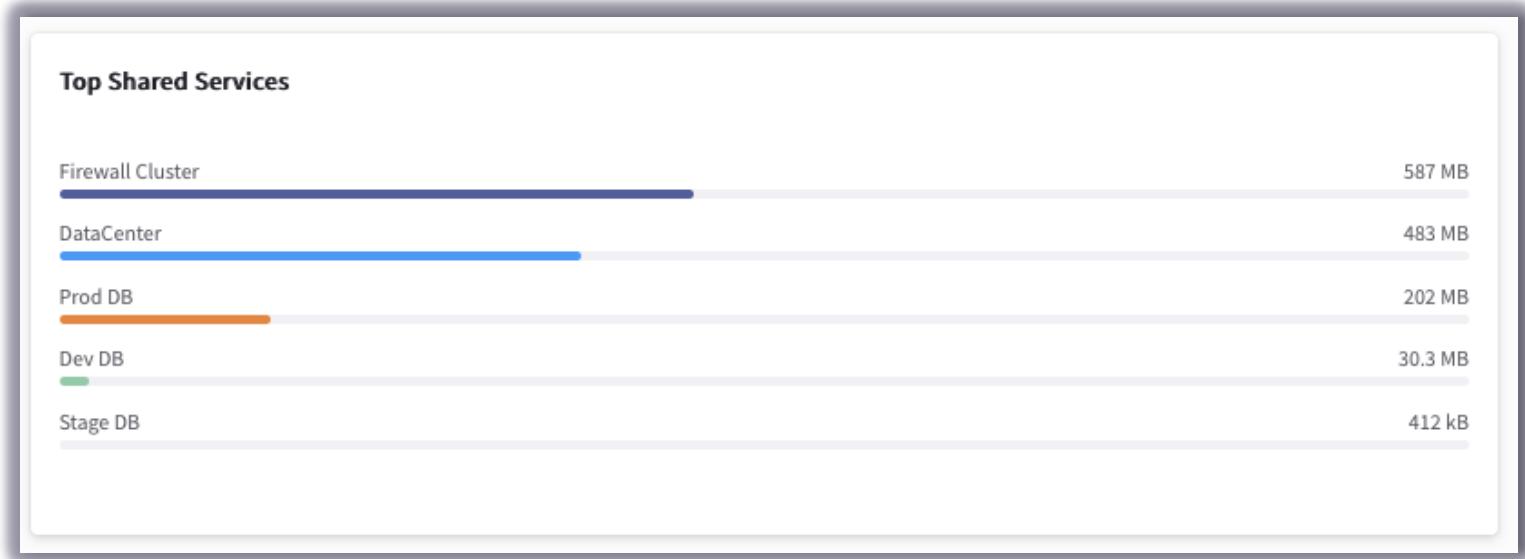
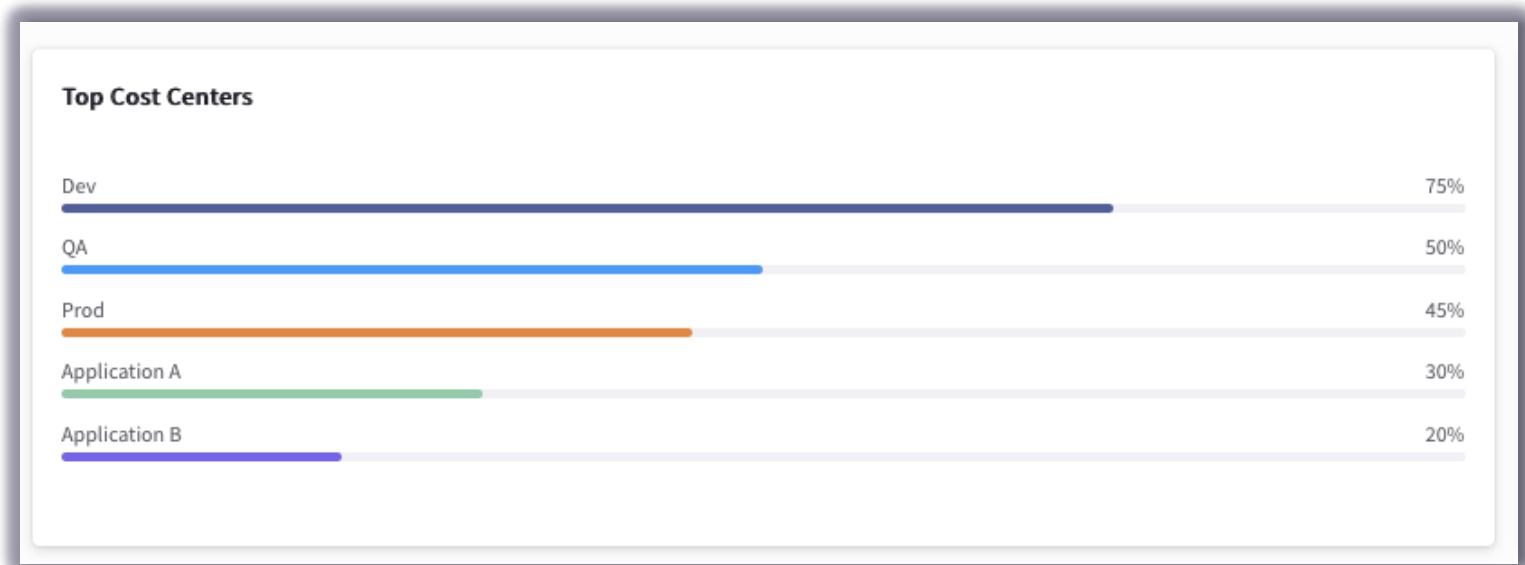
MONITORING THE COST OF YOUR BUSINESS UNITS

ACE Team

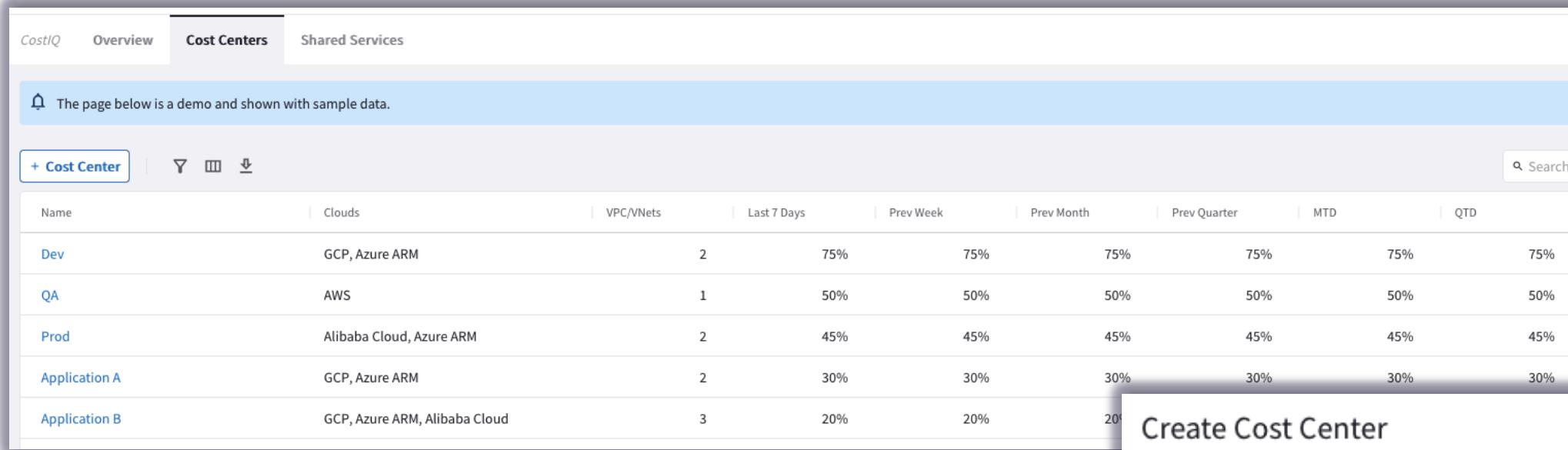


# What is it?

- The **CostIQ** feature provides detailed traffic distribution analysis for your cost centers, including traffic flowing to shared-service resource hosts by Cloud Account, by Cost Center, by VPC/VNet, and by Gateway.
- The cost information displayed in CostIQ is grouped by:
  - Cost Center** - A group of resources categorized by CSP (Cloud Service Provider) tags, associated VPCs/VNets. These CoPilot Cost Centers contain resources used by your real-life cost centers or business units.
  - Shared Service** - A cloud or network resource shared by multiple teams or cost centers. You define Shared Services by listing the IP addresses or IP CIDR ranges of the shared resource hosts.



# Cost Center (part.1)



Name	Clouds	VPC/VNets	Last 7 Days	Prev Week	Prev Month	Prev Quarter	MTD	QTD
Dev	GCP, Azure ARM	2	75%	75%	75%	75%	75%	75%
QA	AWS	1	50%	50%	50%	50%	50%	50%
Prod	Alibaba Cloud, Azure ARM	2	45%	45%	45%	45%	45%	45%
Application A	GCP, Azure ARM	2	30%	30%	30%	30%	30%	30%
Application B	GCP, Azure ARM, Alibaba Cloud	3	20%	20%	20%	20%	20%	20%

- The **Cost Center** is a logical grouping that represents a Line of Business or a department. Essentially, the Cost Center can embrace multiple VPCs/VNets across multiple clouds and multiple accounts.

### Create Cost Center

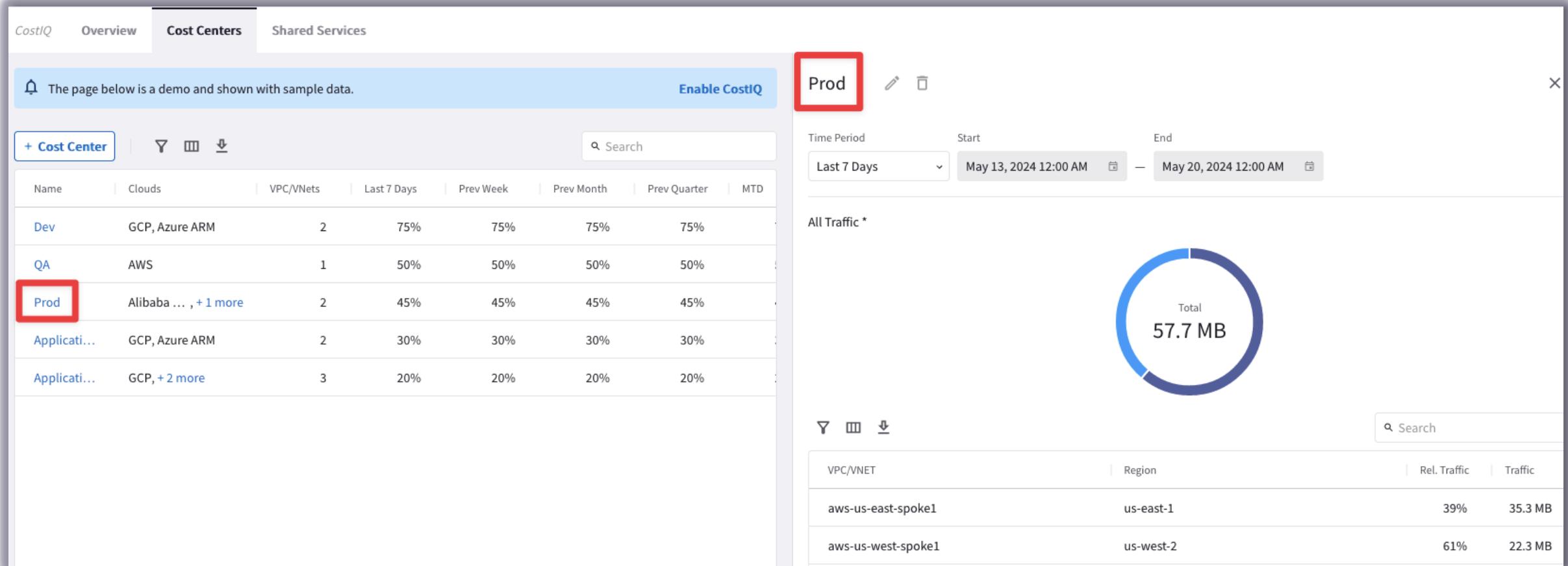
Name: TEST

Associate VPC/VNets:

- aws-us-east-1-spoke1
- aws-us-east-2-spoke1

[Cancel](#) [Save](#)

# Cost Center (part.2)



The screenshot shows the Aviatrix Cost Center interface. At the top, there are tabs for 'CostIQ', 'Overview', 'Cost Centers' (which is selected), and 'Shared Services'. A message at the top left states: 'The page below is a demo and shown with sample data.' There is a button 'Enable CostIQ' on the right.

The main area displays a table of cost centers. One row for 'Prod' is highlighted with a red box. The table includes columns for Name, Clouds, VPC/VNets, and various percentage metrics (Last 7 Days, Prev Week, Prev Month, Prev Quarter, MTD). The 'Prod' row shows Alibaba and AWS as clouds, with 2 VPC/VNets, 45% traffic, and 57.7 MB total traffic.

To the right of the table, a section titled 'Prod' is expanded. It shows a time period from 'Last 7 Days' (May 13, 2024 to May 20, 2024) and a circular donut chart labeled 'Total 57.7 MB' representing all traffic. Below the chart is a table showing traffic distribution by VPC/VNET and Region:

VPC/VNET	Region	Rel. Traffic	Traffic
aws-us-east-spoke1	us-east-1	39%	35.3 MB
aws-us-west-spoke1	us-west-2	61%	22.3 MB

- After defined a Cost Center, you can investigate all the associated Application VPCs/VNets that are all part of that Cost Center. You can drill down and find out the **relative amount of traffic** for each Application VPC/Vnet.

# Shared Center (part.1)

Name	IP or CIDRs	Last 7 Days	Prev Week	Prev Month	Prev Quarter	MTD	QTD
Firewall Cluster	10.11.1.0	587 MB	587 MB	587 MB	587 MB	587 MB	587 MB
Data Center	11.100.0.0/24	483 MB	483 MB	483 MB	483 MB	483 MB	483 MB
Prod DB	120.20.0.24	202 MB	202 MB	202 MB	202 MB	202 MB	202 MB
Dev DB	10.21.1.89, 10.21.1.50, 10.21.1.10	30.3 MB	30.3 MB	30.3 MB	30.3 MB	30.3 MB	30.3 MB
Stage DB	10.21.1.90	412 kB	412 kB				

### Add Shared Service

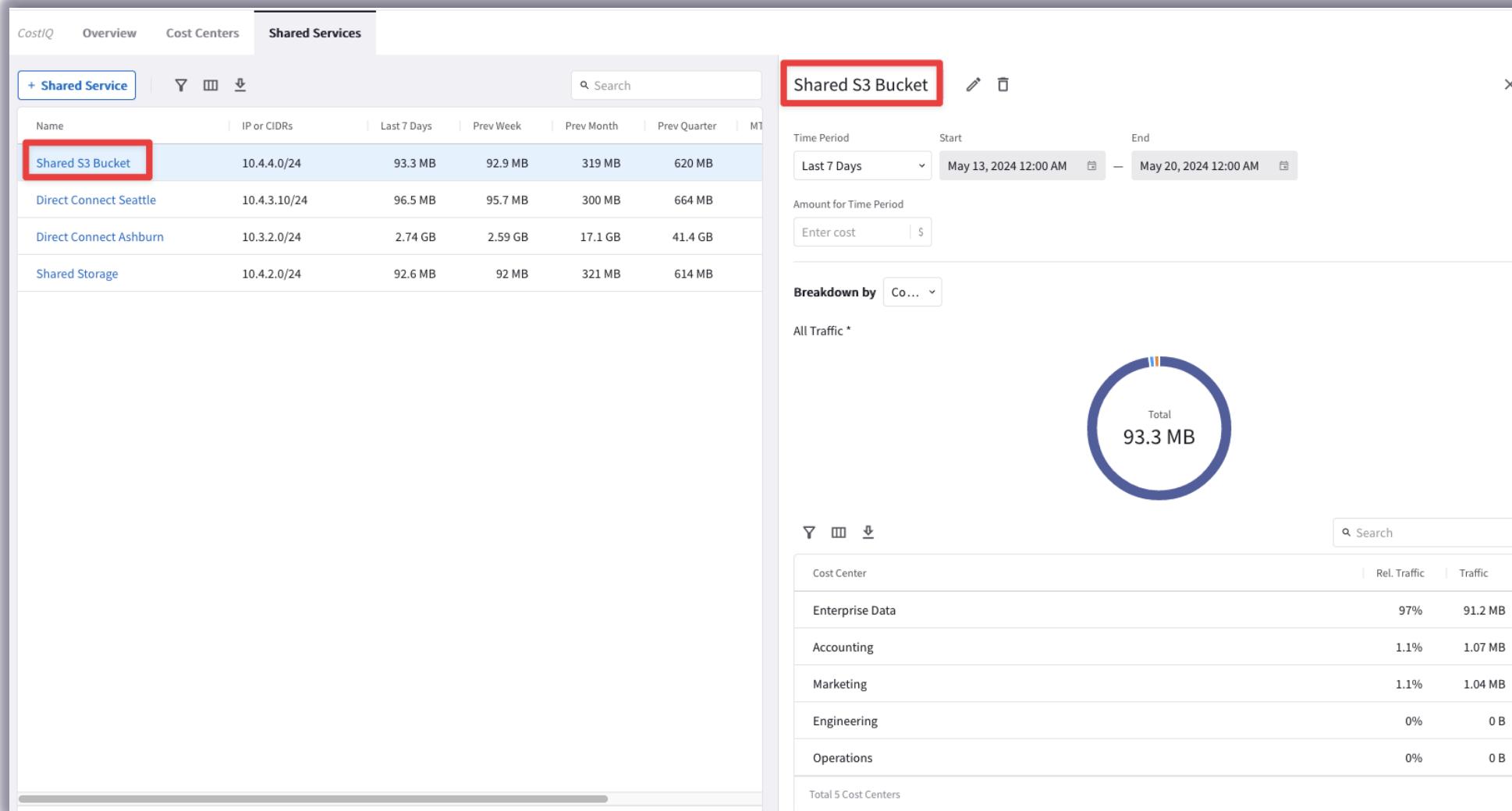
Name:

IP CIDRs:  X

[Cancel](#) [Save](#)

- The **Shared Service** is another logical grouping that represents a Shared Application, for instance a syslog collector like Splunk. You can also associate S3 buckets to your Shared Services.
- The Shared Service allows you to monitor the resources that try reaching your shared applications

# Shared Center (part.2)



The screenshot shows the Aviatrix CostIQ interface. The main navigation bar includes 'CostIQ', 'Overview', 'Cost Centers', and 'Shared Services'. The 'Shared Services' tab is selected, highlighted by a red border. Below this, a table lists various shared services with their IP ranges, traffic volumes, and costs. A row for 'Shared S3 Bucket' is highlighted with a red box. A modal window titled 'Shared S3 Bucket' provides more details about this specific service. The modal includes a time period selector set to 'Last 7 Days' from May 13 to May 20, 2024. It also features a breakdown by cost center. A large circular chart in the center of the modal displays a total traffic volume of 93.3 MB. Below the chart, a table lists the traffic distribution across five cost centers: Enterprise Data (97%, 91.2 MB), Accounting (1.1%, 1.07 MB), Marketing (1.1%, 1.04 MB), Engineering (0%, 0 B), and Operations (0%, 0 B).

Name	IP or CIDRs	Last 7 Days	Prev Week	Prev Month	Prev Quarter
Shared S3 Bucket	10.4.4.0/24	93.3 MB	92.9 MB	319 MB	620 MB
Direct Connect Seattle	10.4.3.10/24	96.5 MB	95.7 MB	300 MB	664 MB
Direct Connect Ashburn	10.3.2.0/24	2.74 GB	2.59 GB	17.1 GB	41.4 GB
Shared Storage	10.4.2.0/24	92.6 MB	92 MB	321 MB	614 MB

Cost Center	Rel. Traffic	Traffic
Enterprise Data	97%	91.2 MB
Accounting	1.1%	1.07 MB
Marketing	1.1%	1.04 MB
Engineering	0%	0 B
Operations	0%	0 B
Total 5 Cost Centers		

- After defining a **Shared Service**, you can accurately find out what LOB/Department has been utilizing it.



Next: Lab 9 – Threat Prevention &  
Lab 10 - CostIQ