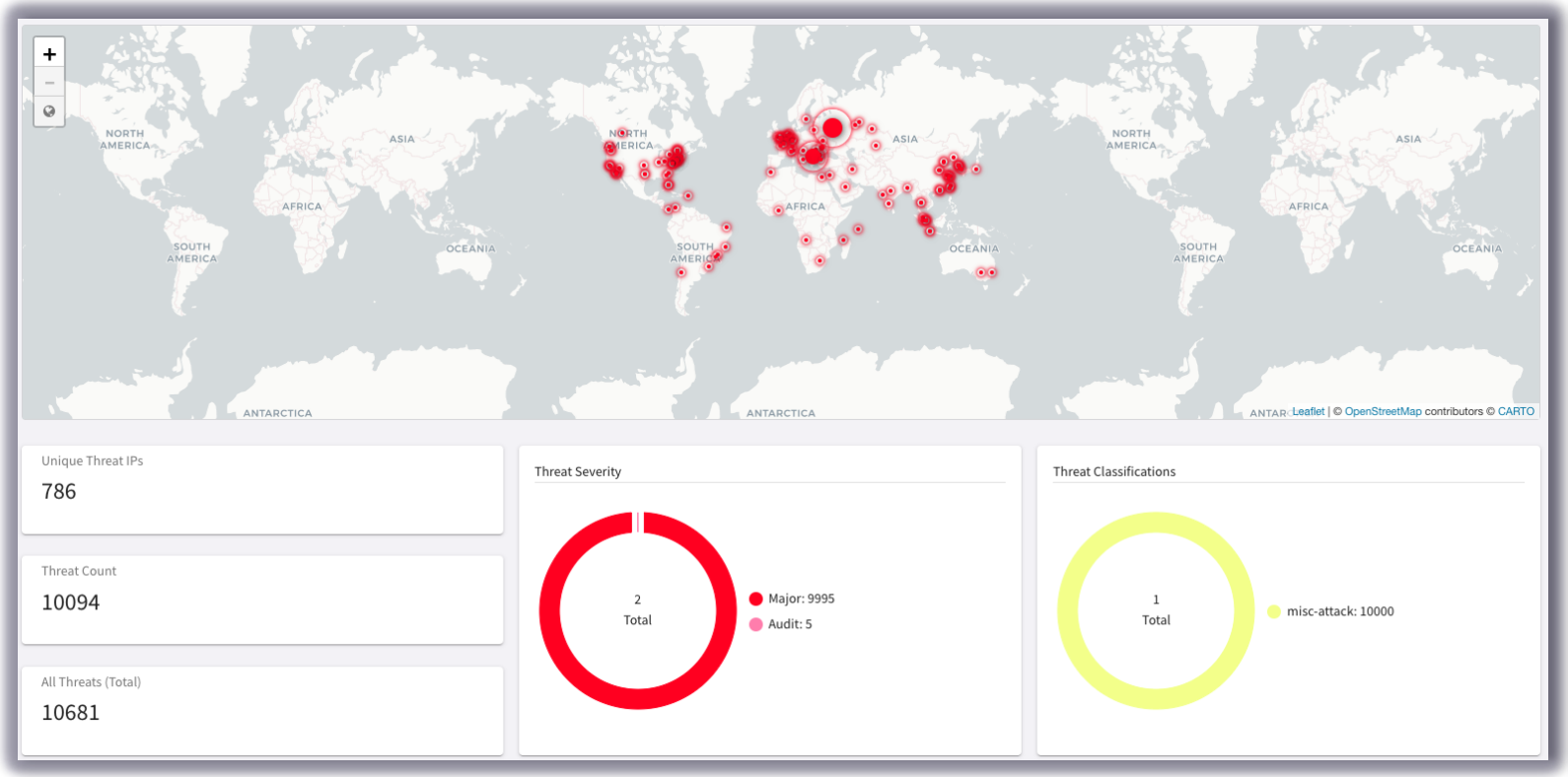
Threat Prevention

IDENTIFY AND REMEDIATE THREATS ACROSS MULTICLOUD NETWORKS

ACE Solutions Architecture Team

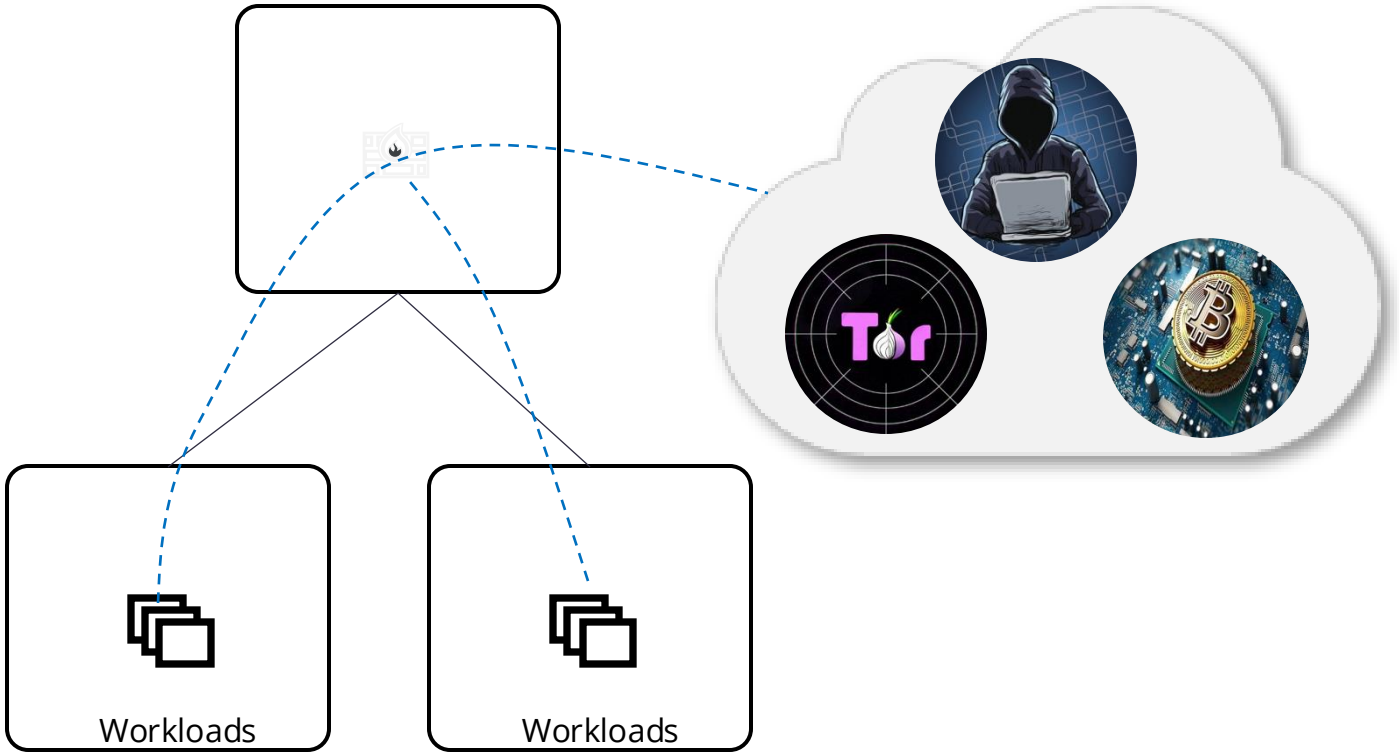
What is it?

- 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

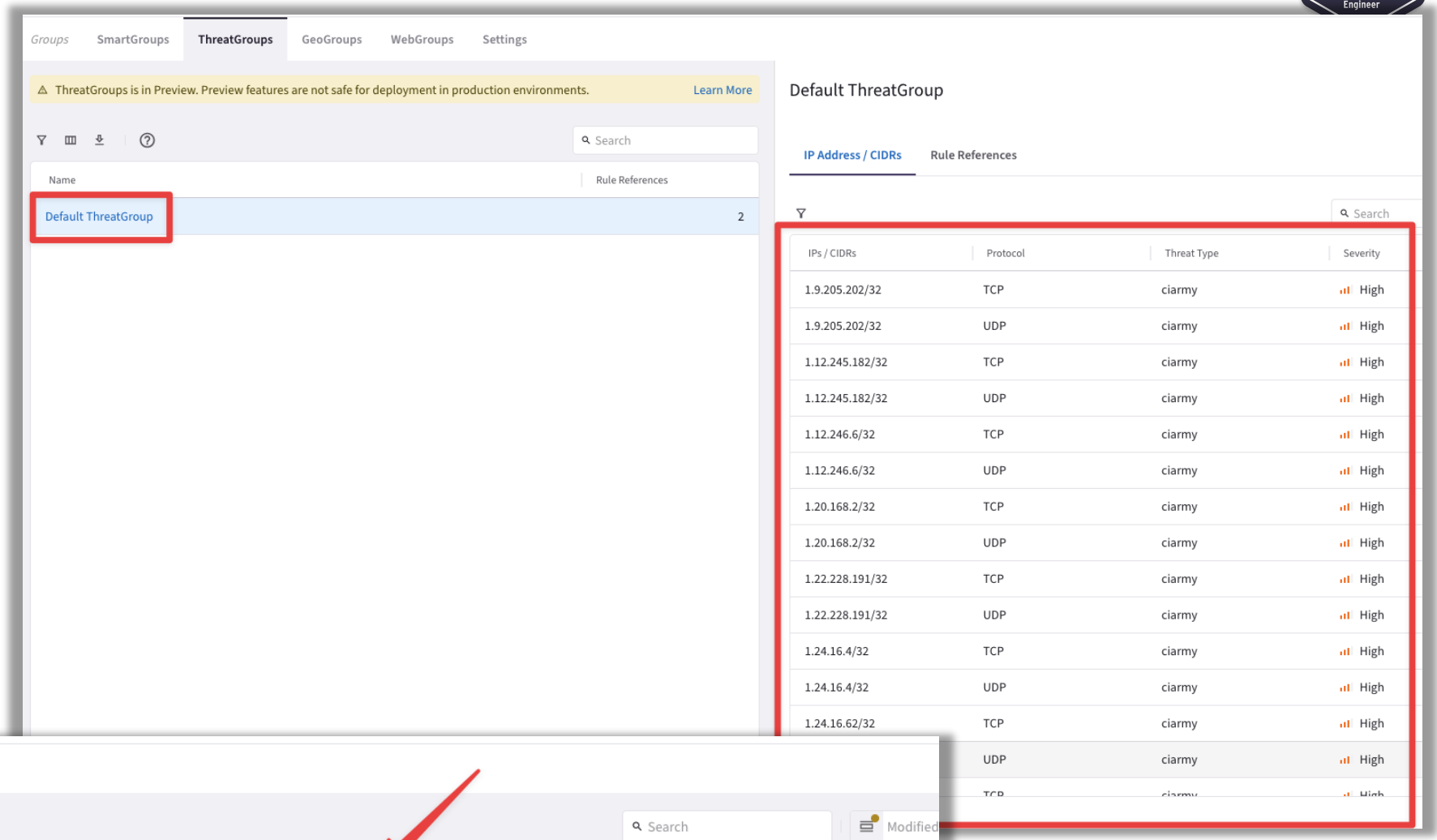


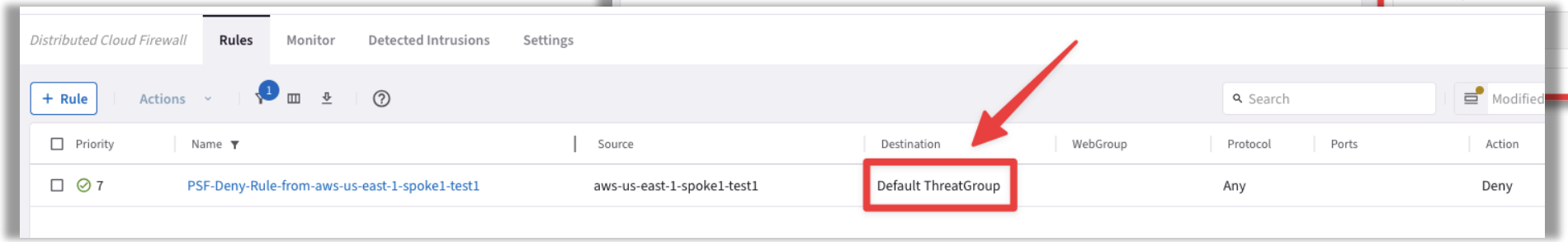
Default ThreatGroup

- **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

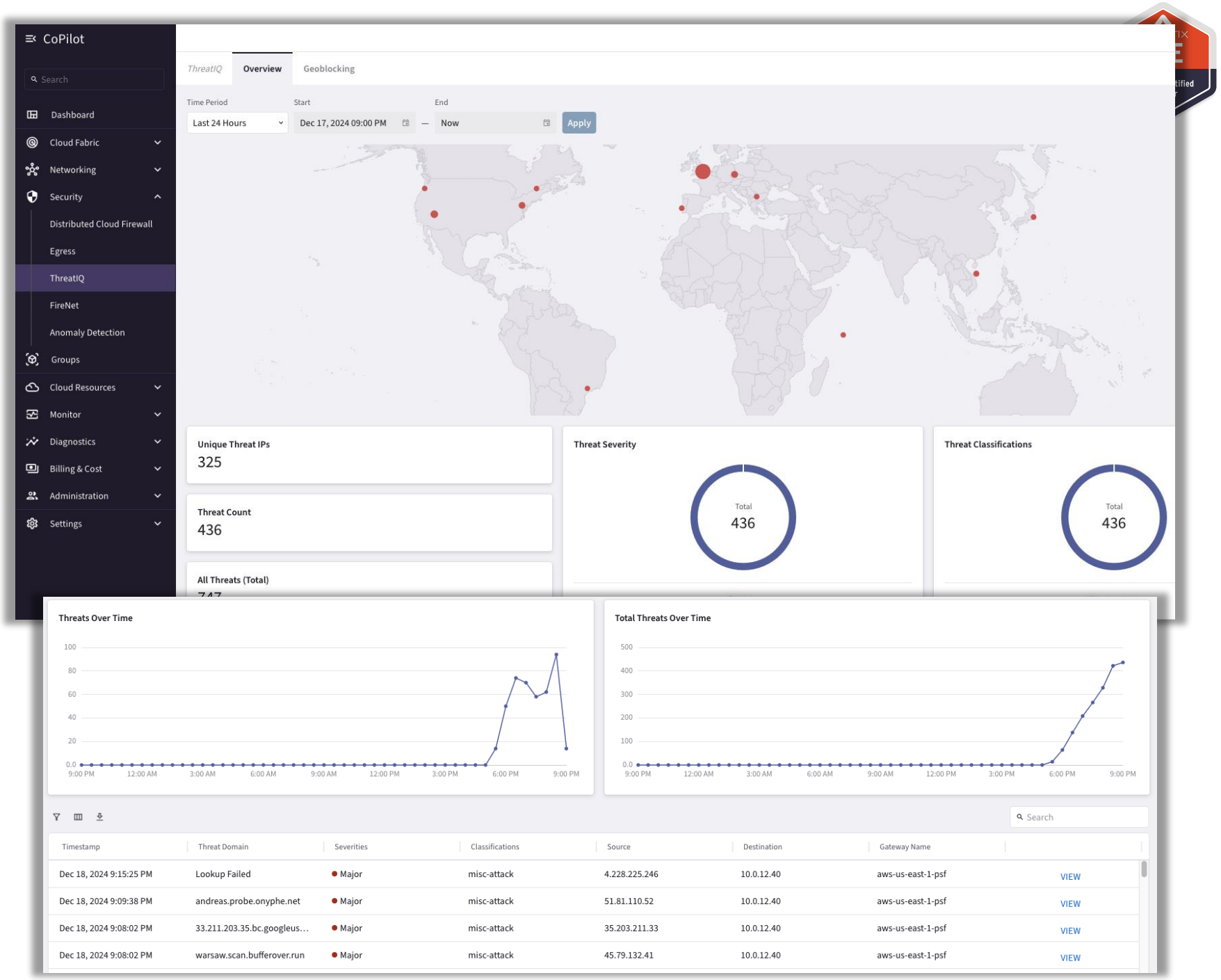




ThreatIQ

- **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).

- **Geoblocking Tab**
  - Block traffic coming from other countries



aviatrix

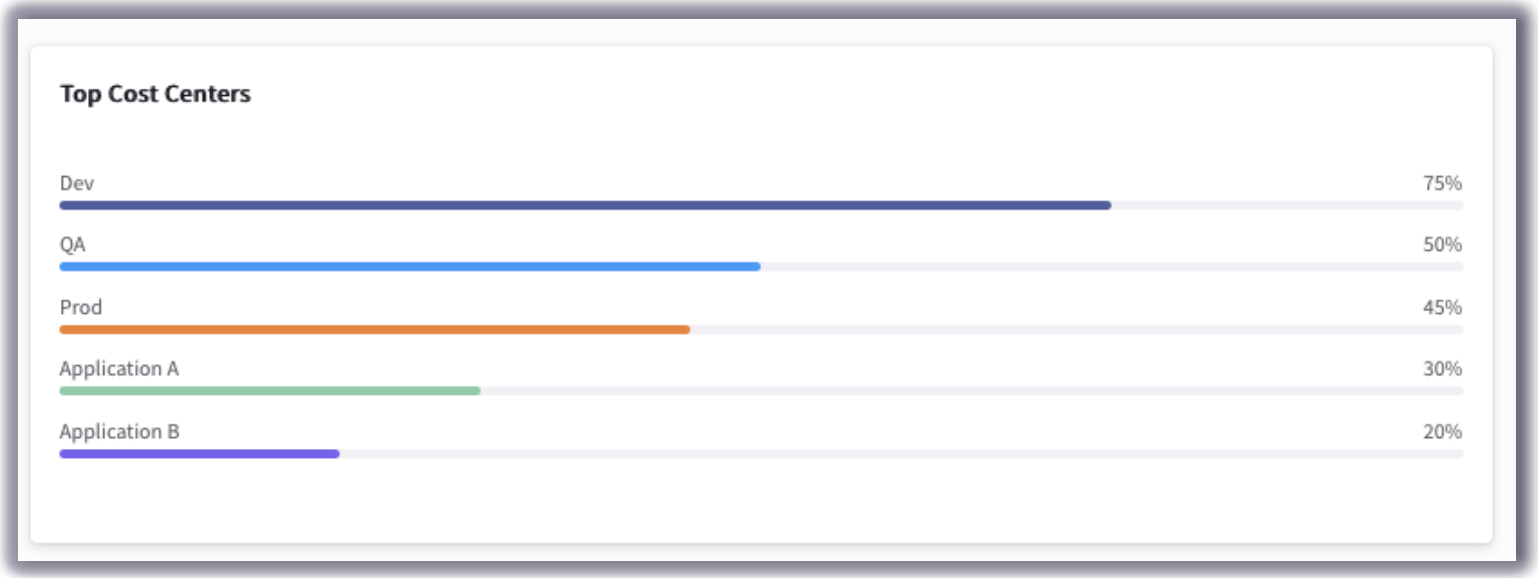
CostIQ

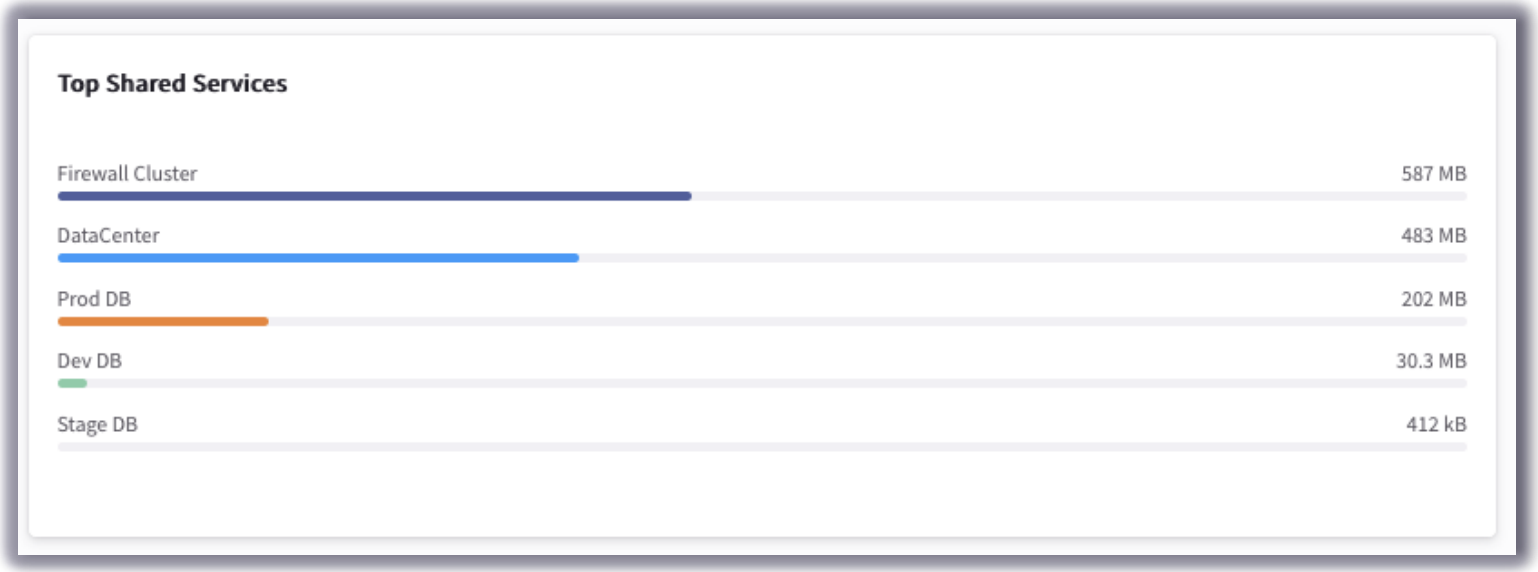
MONITORING THE COST OF YOUR BUSINESS UNITS

ACE Solutions Architecture 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)

CostIQ | Overview | Cost Centers | Shared Services

The page below is a demo and shown with sample data.

+ Cost Center

Search

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%			

Create Cost Center

Name

TEST

Associate VPC/VNets

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

Cancel Save

- 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.

Cost Center (part.2)

CostIQ | Overview | Cost Centers | Shared Services

The page below is a demo and shown with sample data. Enable CostIQ

+ Cost Center

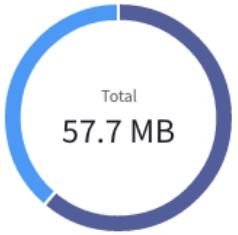
Search

Name	Clouds	VPC/VNets	Last 7 Days	Prev Week	Prev Month	Prev Quarter	MTD
Dev	GCP, Azure ARM	2	75%	75%	75%	75%	
QA	AWS	1	50%	50%	50%	50%	
Prod	Alibaba ... , + 1 more	2	45%	45%	45%	45%	
Applicati...	GCP, Azure ARM	2	30%	30%	30%	30%	
Applicati...	GCP, + 2 more	3	20%	20%	20%	20%	

Prod

Time Period: Last 7 Days | Start: May 13, 2024 12:00 AM | End: May 20, 2024 12:00 AM

All Traffic *



Search

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)

+ Shared Service

Search

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

SPLUNK

IP CIDRs

10.11.150.28

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)

CostIQ | Overview | Cost Centers | Shared Services

+ Shared Service | Search

Name	IP or CIDRs	Last 7 Days	Prev Week	Prev Month	Prev Quarter	MT
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	

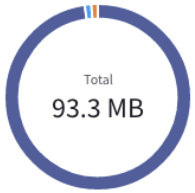
Shared S3 Bucket

Time Period: Last 7 Days | Start: May 13, 2024 12:00 AM — End: May 20, 2024 12:00 AM

Amount for Time Period: Enter cost $

Breakdown by: Co...

All Traffic *



Search

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