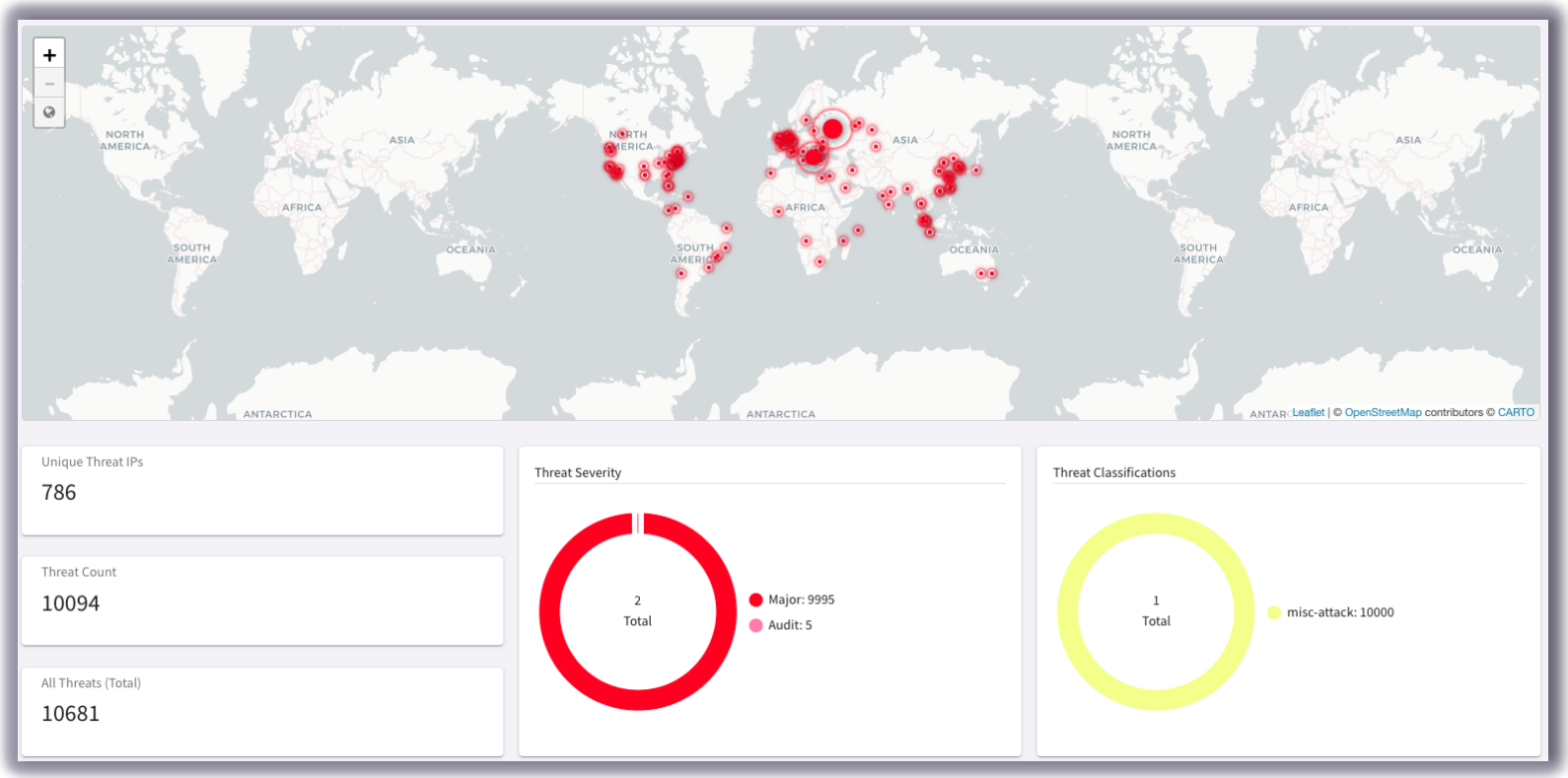
Threat Prevention

IDENTIFY AND REMEDIATE THREATS ACROSS MULTICLOUD NETWORKS

ACE Team

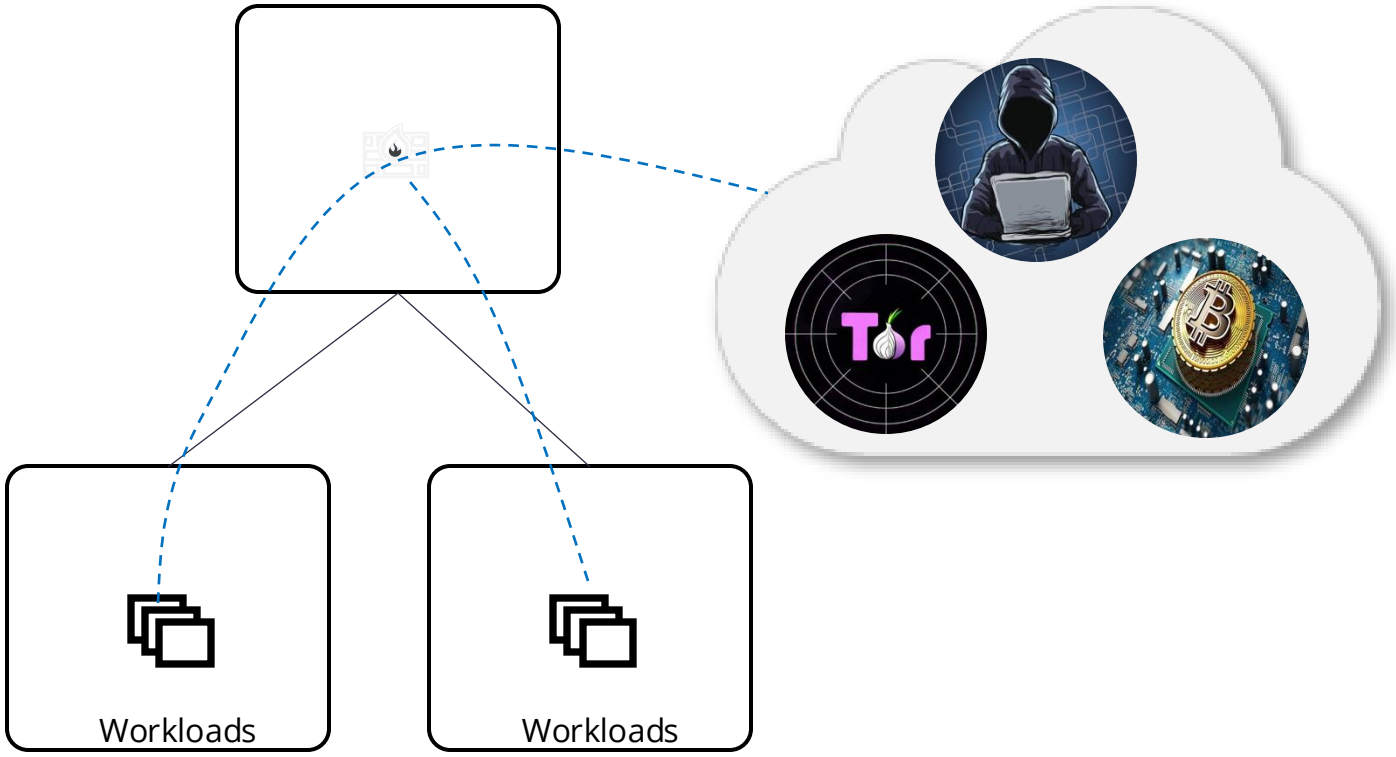
What is it?

- 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



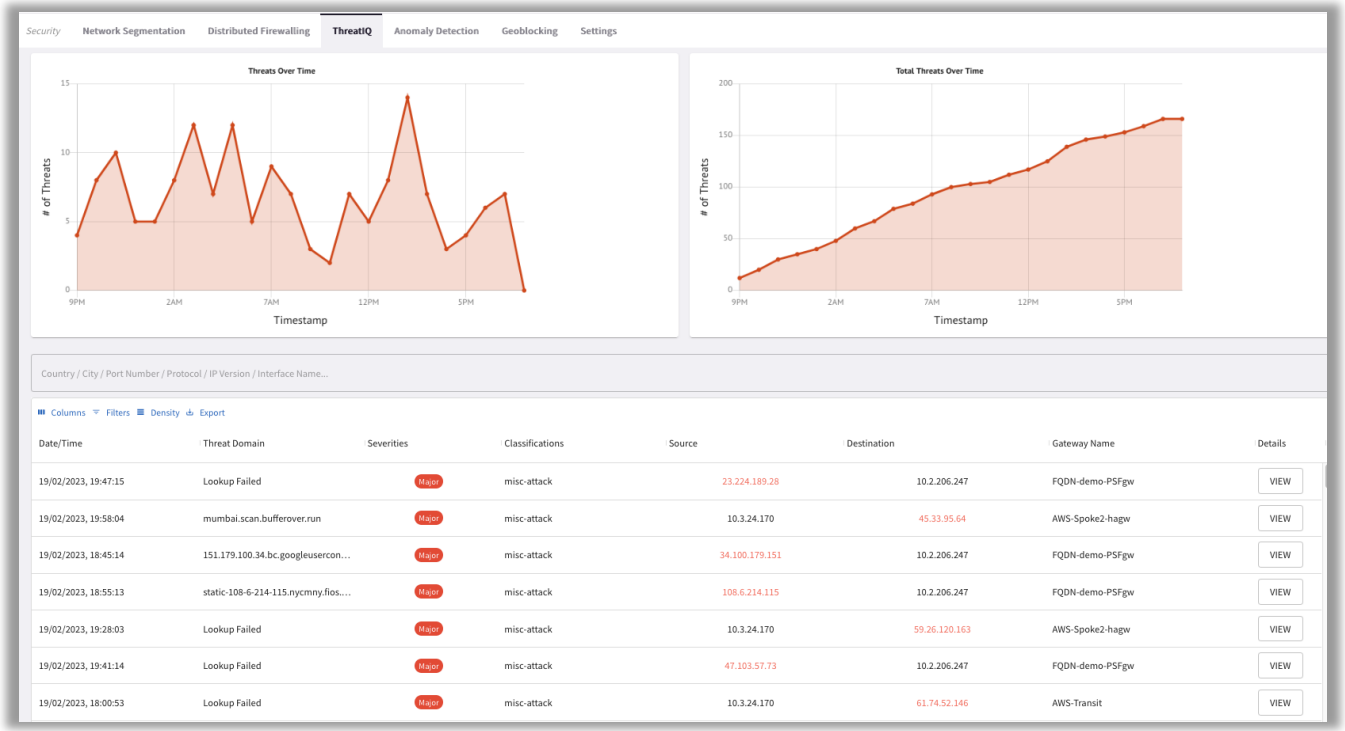
Why should enterprises care about threats?

- 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

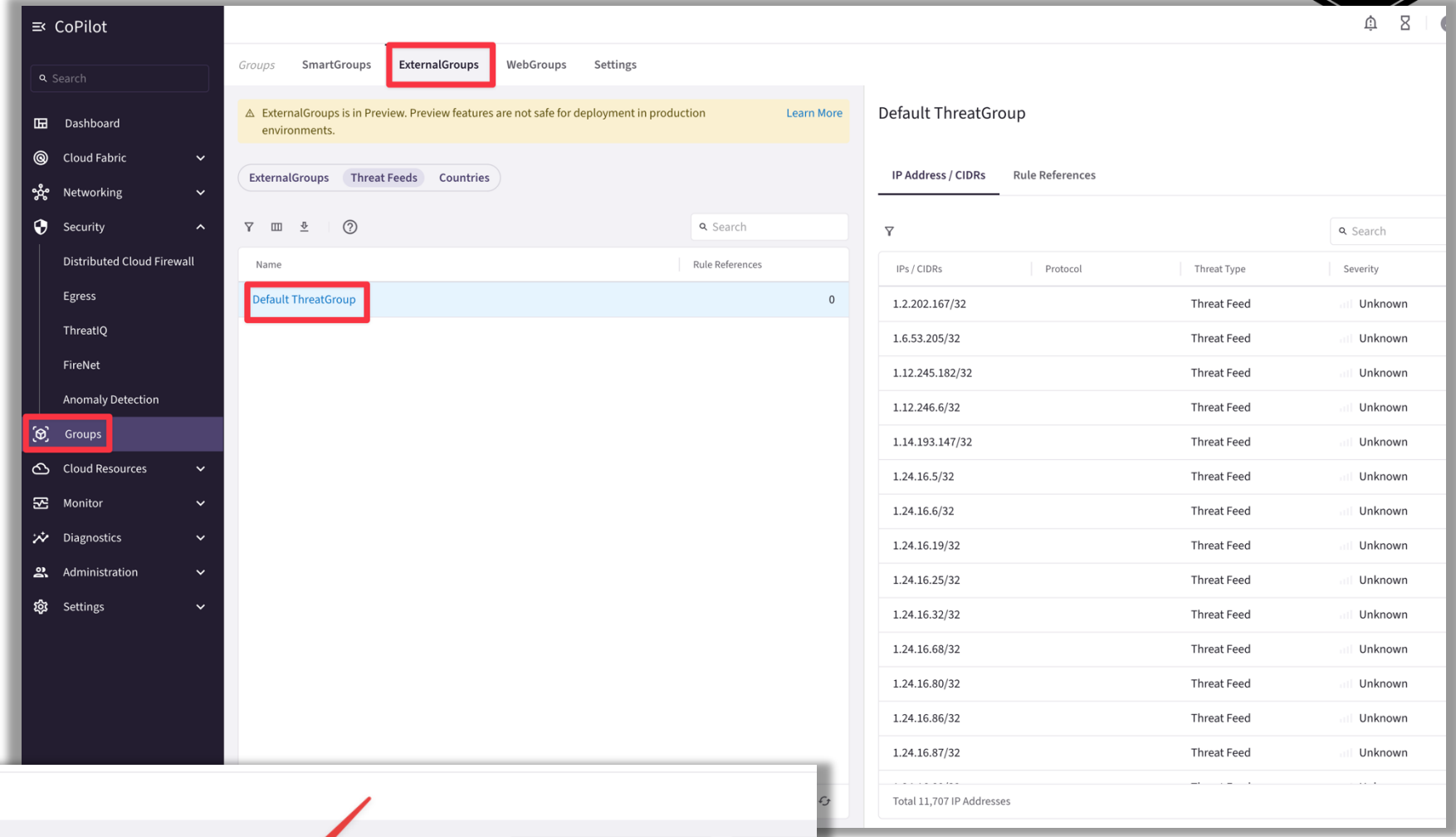


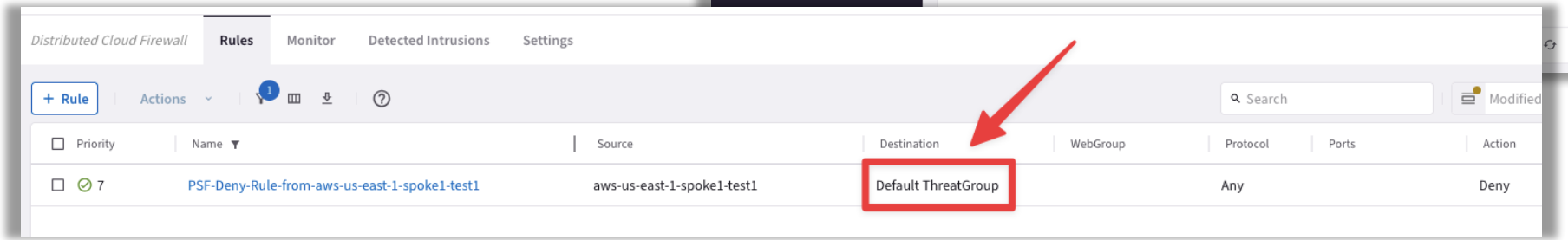
Default ThreatGroup

- **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:**

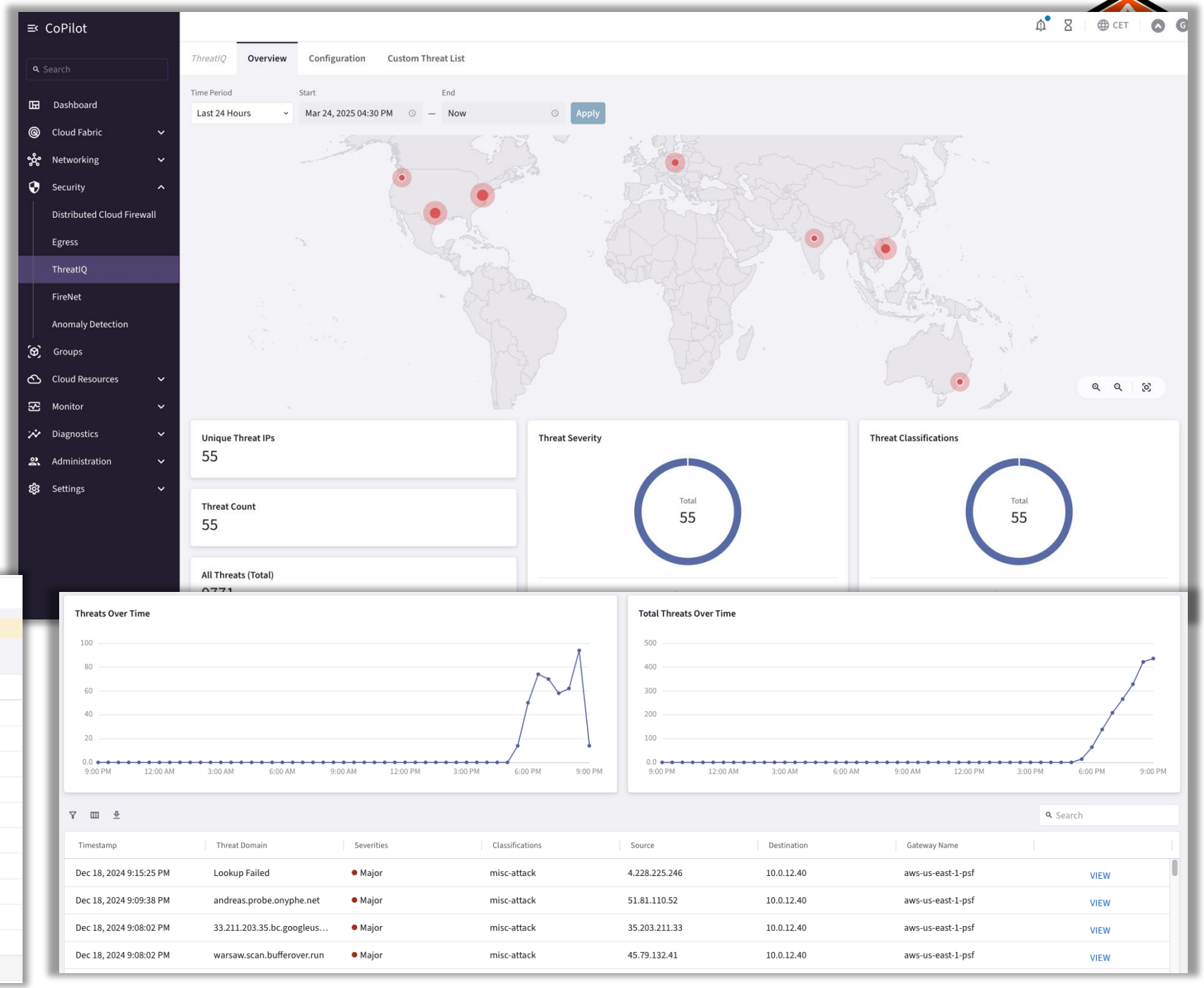
- You cannot have a ThreatGroup as both source and a destination in a DCF rule

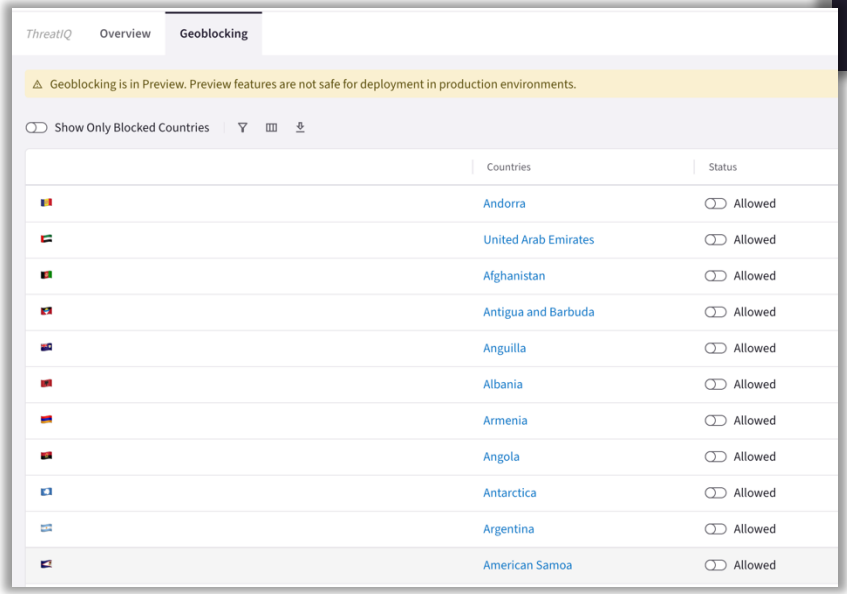




ThreatIQ

- **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





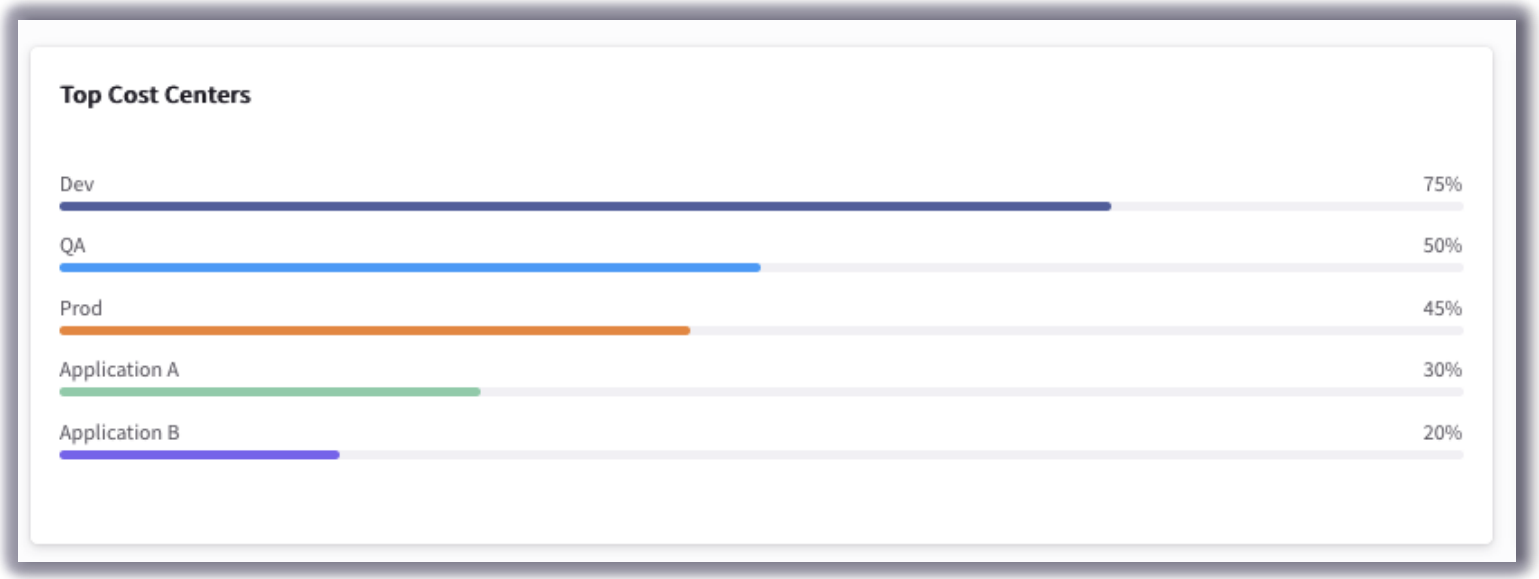
CostIQ

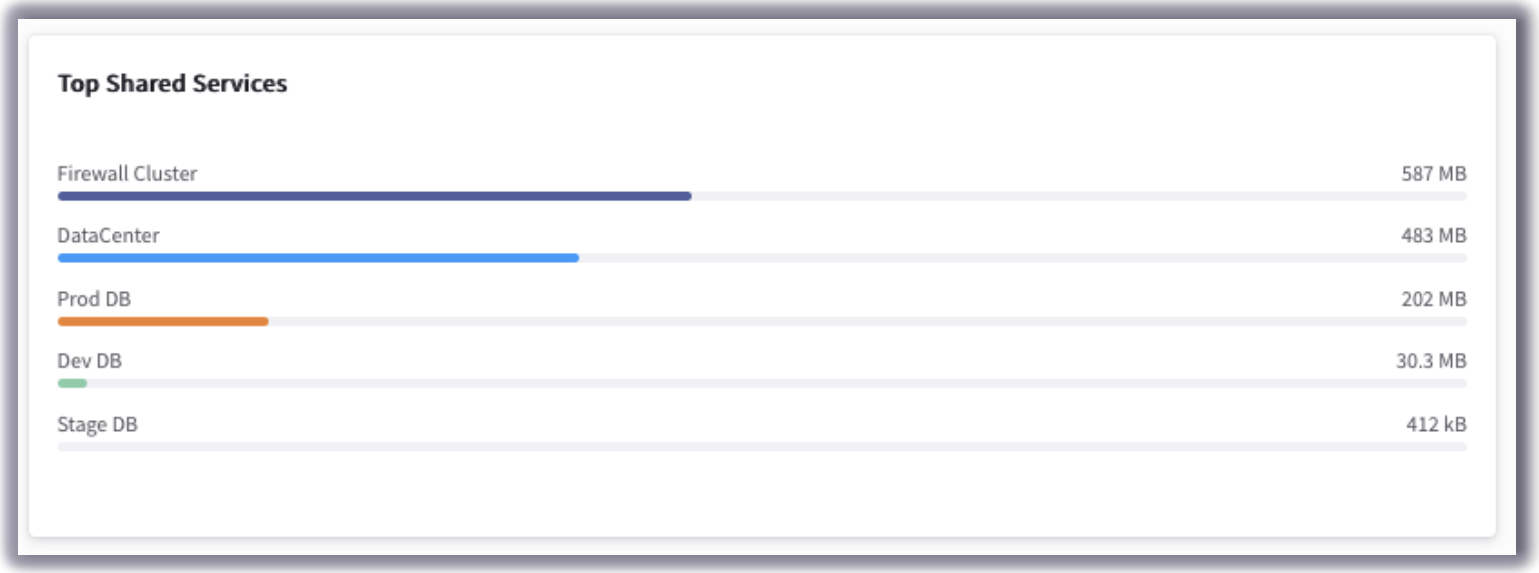
MONITORING THE COST OF YOUR BUSINESS UNITS

ACE Team

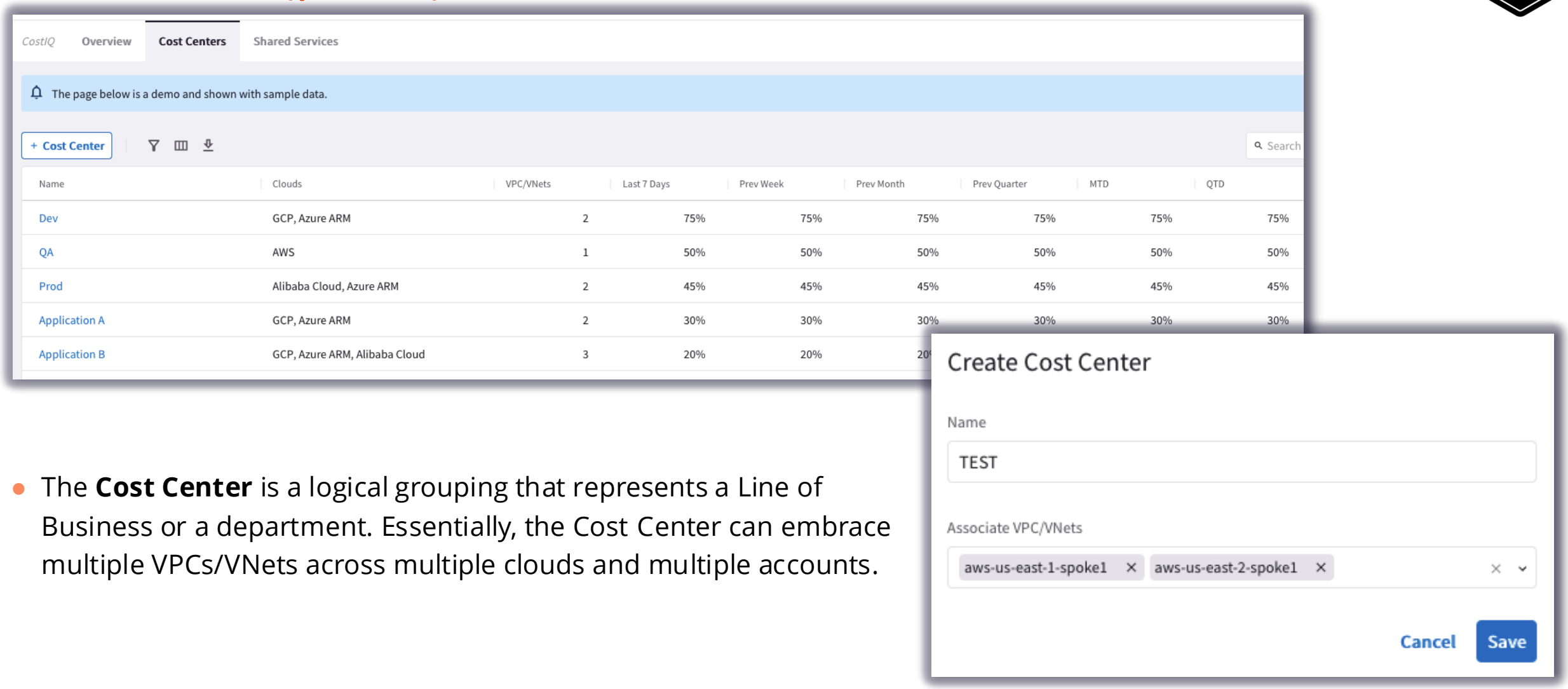
What is it?

- 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.



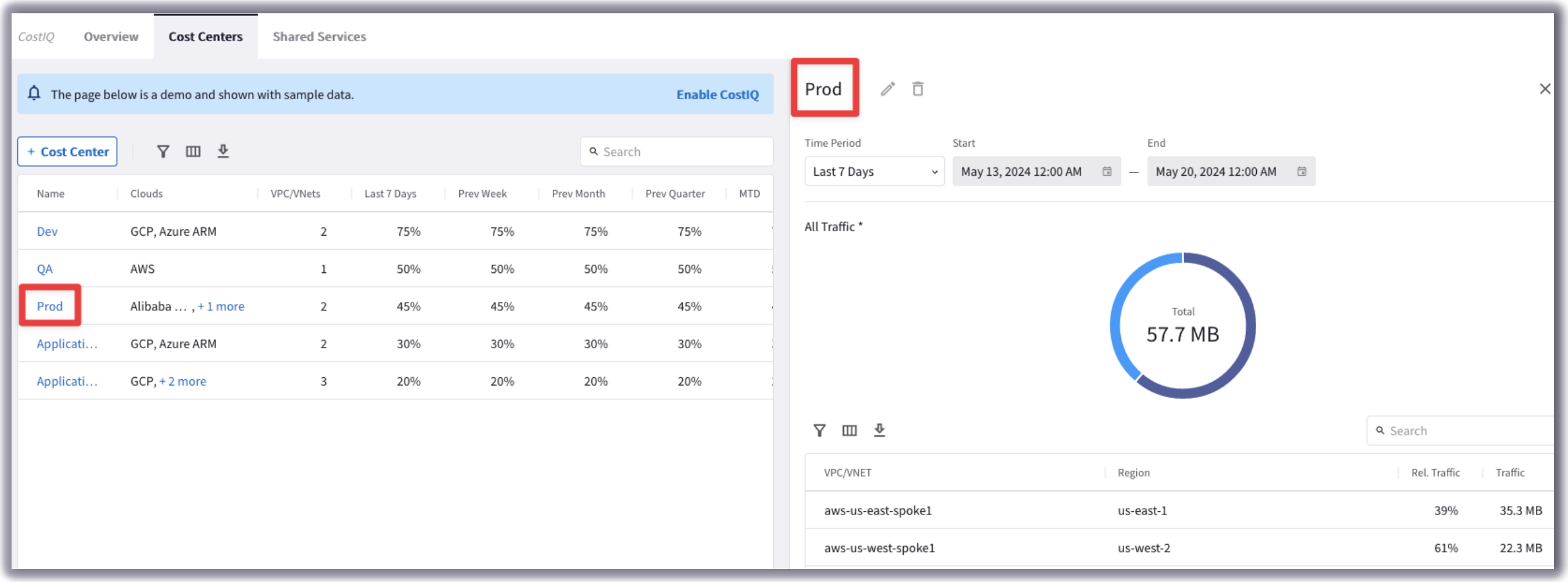


Cost Center (part.1)



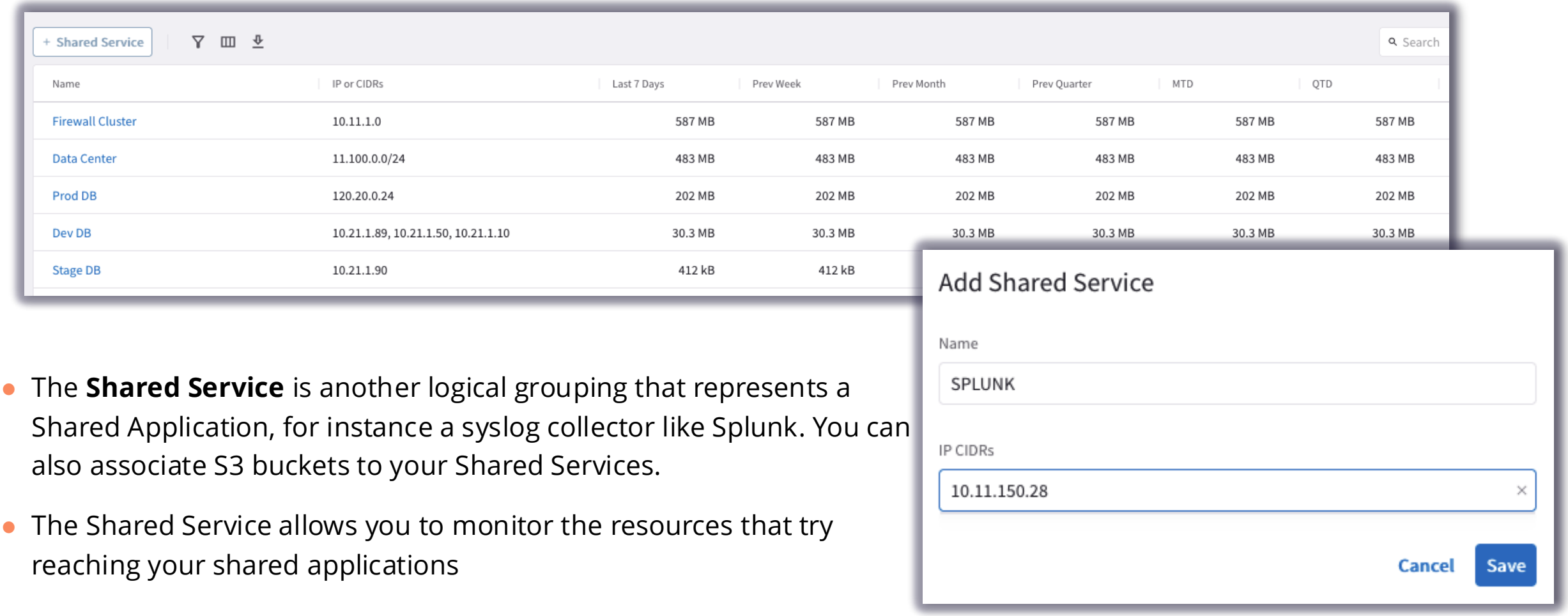
- The **Cost Center** is a logical grouping that represents a Line of Business or a department. Essentially, the Cost Center can embrace multiple VPCs/VNets across multiple clouds and multiple accounts.

Cost Center (part.2)



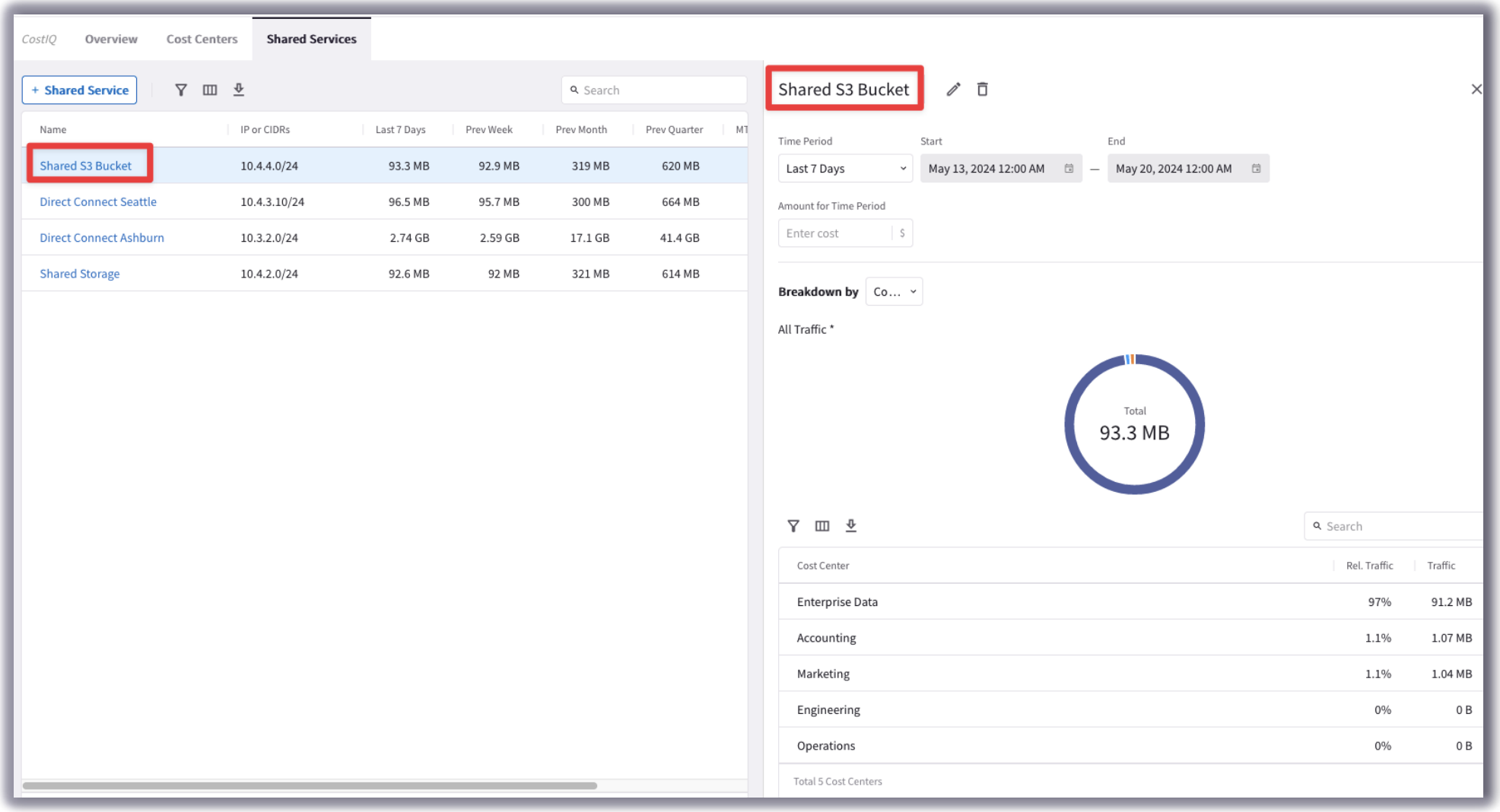
- After defined a Cost Center, you can investigate all the associated Application VPCs/VNets that are all part of that Cost Center. You can drill down and find out the **relative amount of traffic** for each Application VPC/Vnet.

Shared Center (part.1)



- 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)



- 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