AVIATRIX
ACE
SECURITY
SPECIALTY

# ThreatIQ and Anomaly Detection

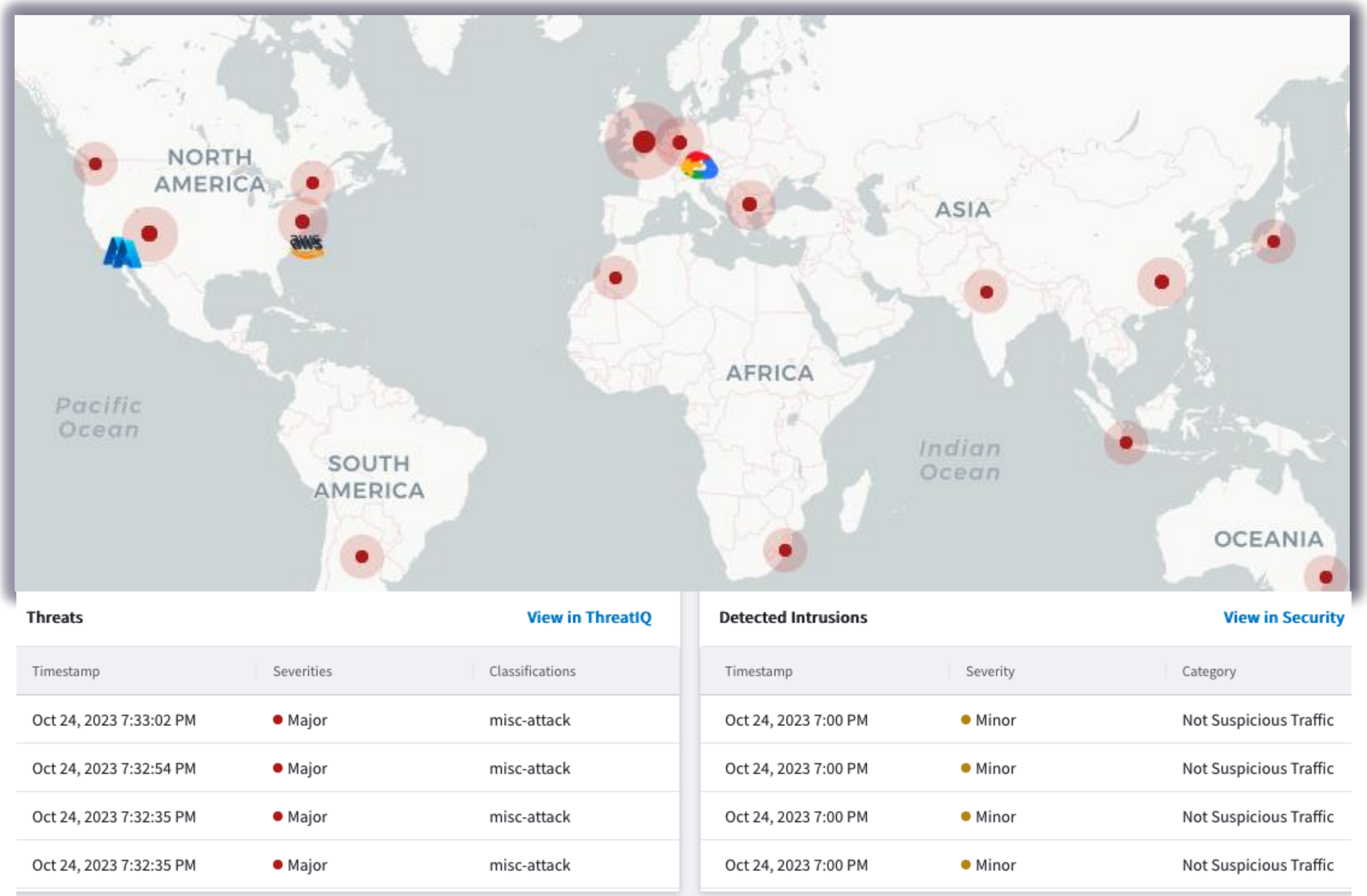
THREATIQ, GEOBLOCKING AND ANOMALY DETECTION

AVIATRIX
ACE
SECURITY
SPECIALTY

# Aviatrix ThreatIQ

# What is it?

- Multicloud native network security to dynamically **identify, alert, and remediate potential threats** to known malicious destinations
- **Distributed threat visibility** and control built into the network data-plane at every hop
- Identify potential **data exfiltration and compromised host**
- **No data-plane performance impact**
- **Complementary security solution** with full multicloud support



**Threats** View in ThreatIQ

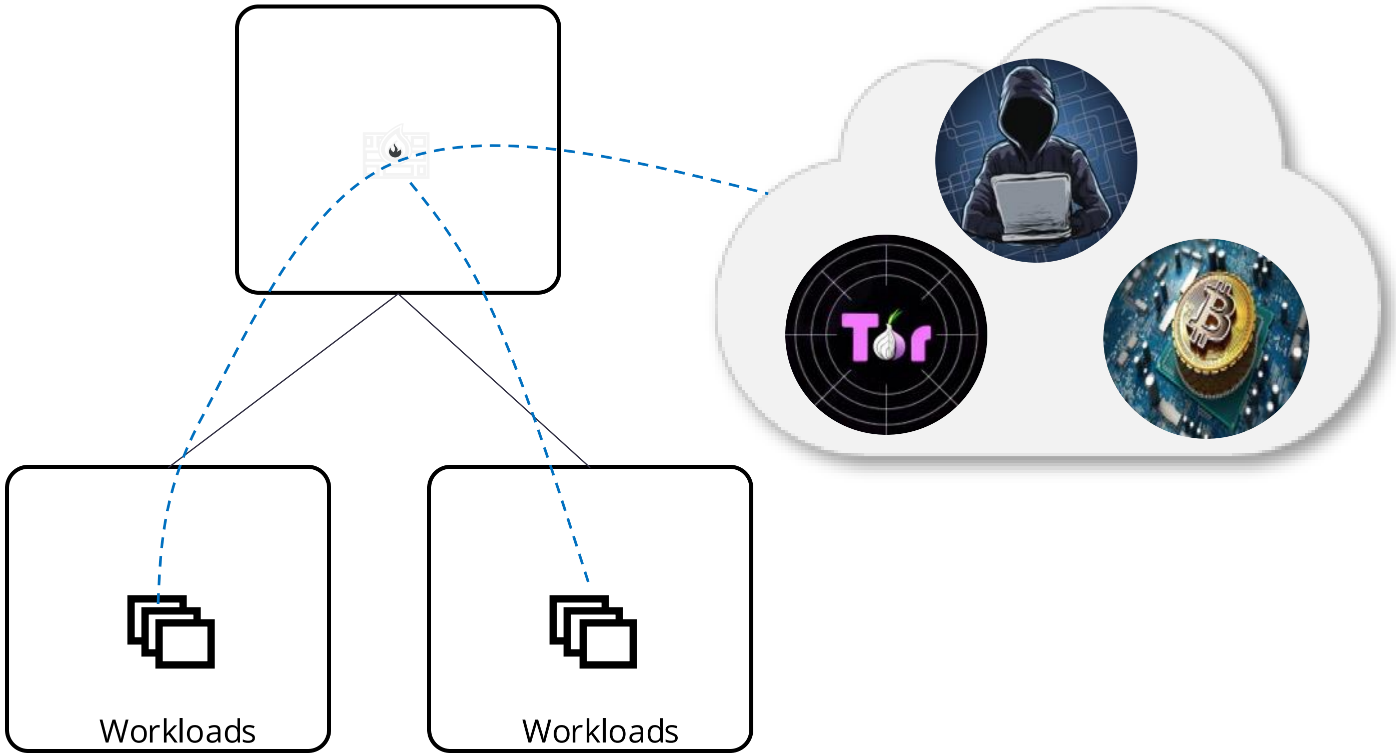
| Timestamp | Severities | Classifications |
|---|---|---|
| Oct 24, 2023 7:33:02 PM | ● Major | misc-attack |
| Oct 24, 2023 7:32:54 PM | ● Major | misc-attack |
| Oct 24, 2023 7:32:35 PM | ● Major | misc-attack |
| Oct 24, 2023 7:32:35 PM | ● Major | misc-attack |

**Detected Intrusions** View in Security

| Timestamp | Severity | Category |
|---|---|---|
| Oct 24, 2023 7:00 PM | ● Minor | Not Suspicious Traffic |
| Oct 24, 2023 7:00 PM | ● Minor | Not Suspicious Traffic |
| Oct 24, 2023 7:00 PM | ● Minor | Not Suspicious Traffic |
| Oct 24, 2023 7:00 PM | ● Minor | Not Suspicious Traffic |

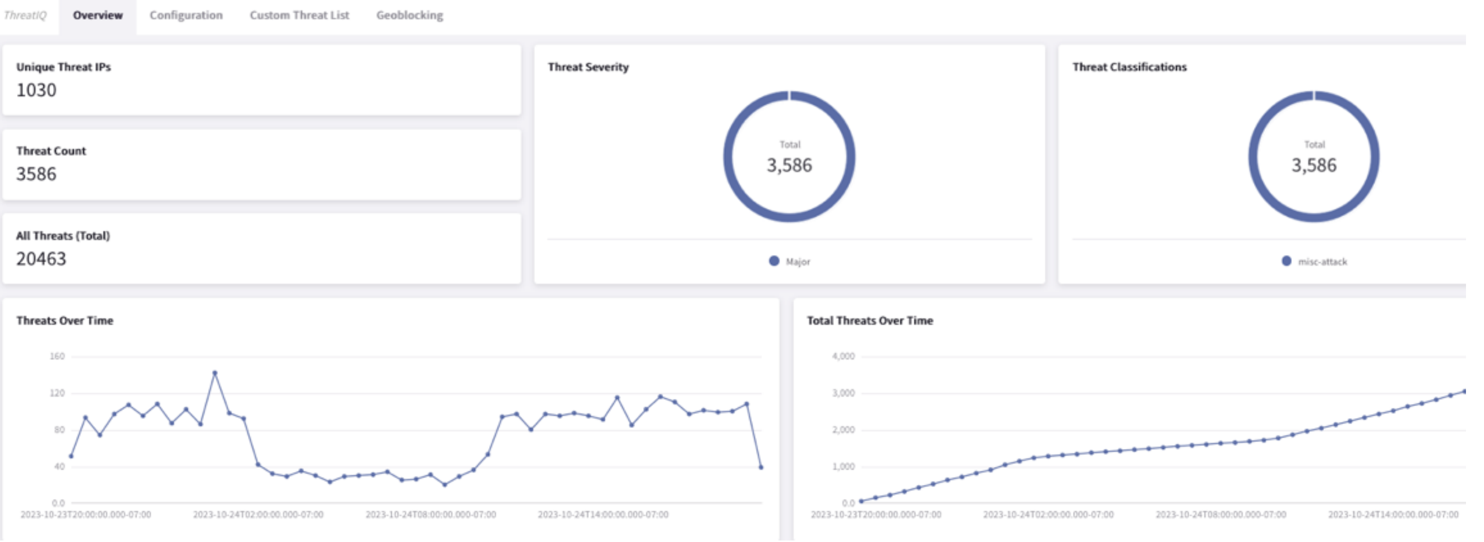
# Why should enterprises care about it?

- 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 to:
  - Data exfiltration
  - Botnets
  - Compromised hosts
  - Crypto mining
  - TOR
  - DDoS, and more



# How does it work?

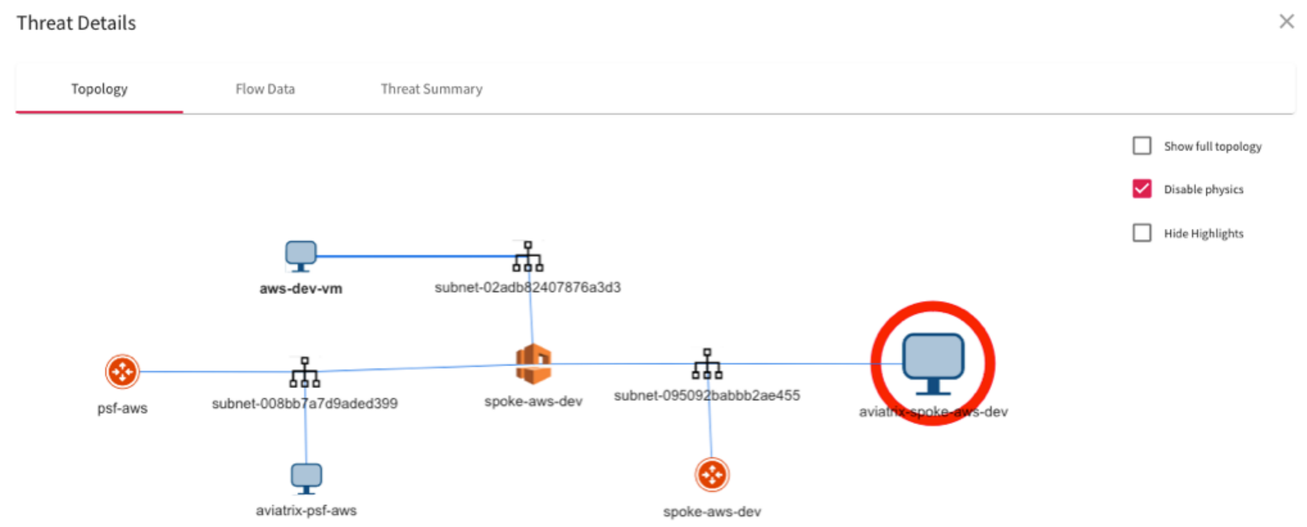
- **Distributed Inspection & Notification**
  - Aviatrix gateways across Multicloud environment send real-time NetFlow data to CoPilot
  - CoPilot analyzes the data on all public destinations against well-known Threat DB
  - CoPilot alerts on any potential threats in the environment
  - CoPilot provides 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


ThreatIQ
Overview
Configuration
Custom Threat List
Geoblocking
Threat Severity
Total
3,586
Major
Threat Classifications
Total
3,586
misc-attack
Threats Over Time
160
120
80
40
0.0
2023-10-23T20:00:00.000-07:00
2023-10-24T02:00:00.000-07:00
2023-10-24T08:00:00.000-07:00
2023-10-24T14:00:00.000-07:00
Total Threats Over Time
4,000
3,000
2,000
1,000
0.0
2023-10-23T20:00:00.000-07:00
2023-10-24T02:00:00.000-07:00
2023-10-24T08:00:00.000-07:00
2023-10-24T14:00:00.000-07:00

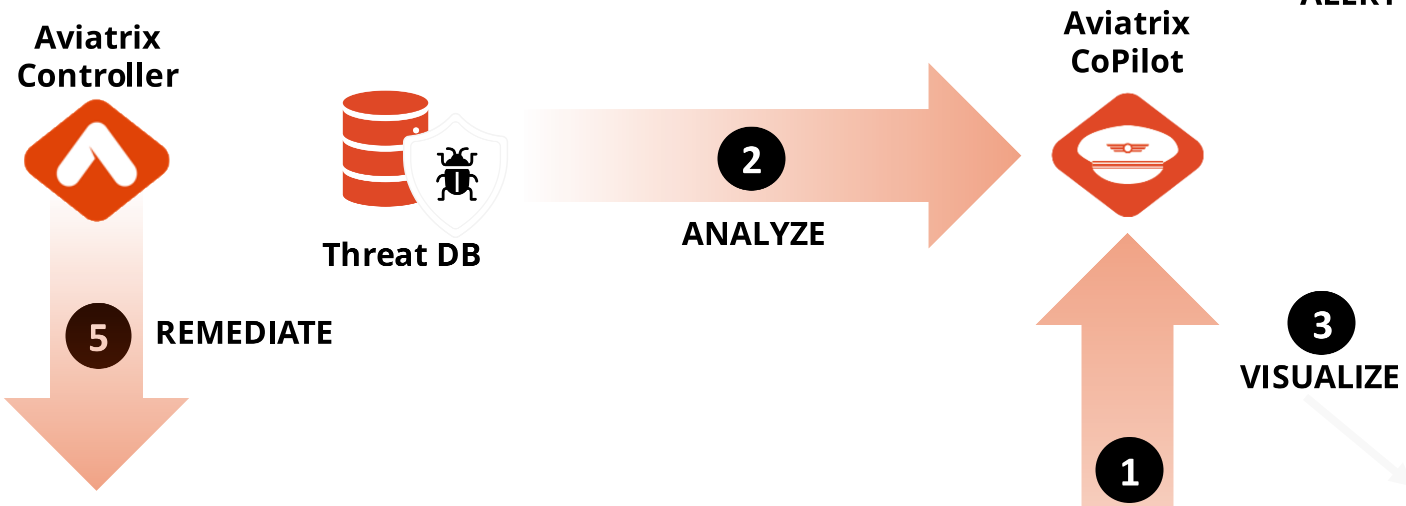
Unique Threat IPs: 1030

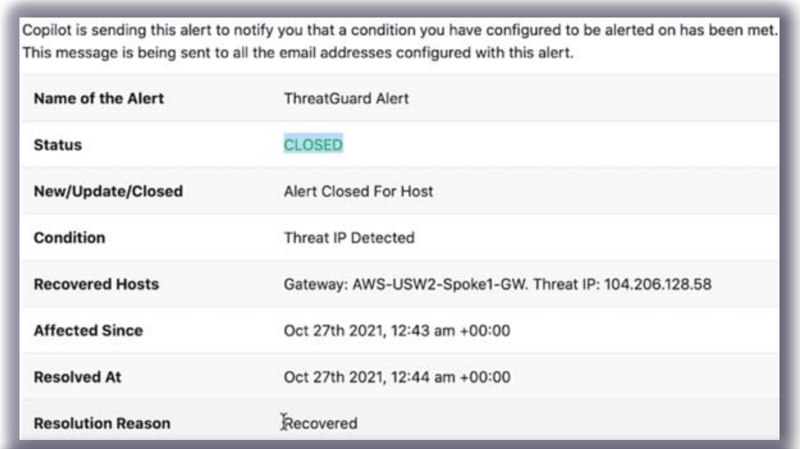
Threat Count: 3586

All Threats (Total): 20463



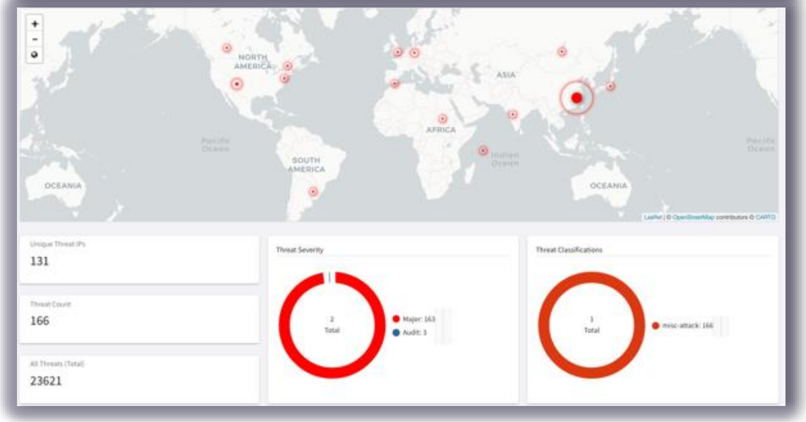
# Workflow



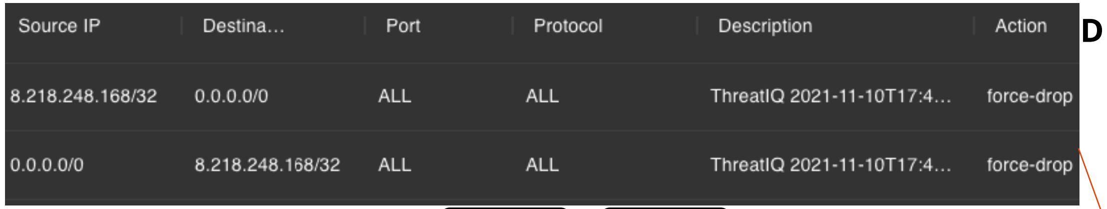


Copilot is sending this alert to notify you that a condition you have configured to be alerted on has been met. This message is being sent to all the email addresses configured with this alert.

| | |
|---|---|
| Name of the Alert | ThreatGuard Alert |
| Status | CLOSED |
| New/Update/Closed | Alert Closed For Host |
| Condition | Threat IP Detected |
| Recovered Hosts | Gateway: AWS-USW2-Spoke1-GW. Threat IP: 104.206.128.58 |
| Affected Since | Oct 27th 2021, 12:43 am +00:00 |
| Resolved At | Oct 27th 2021, 12:44 am +00:00 |
| Resolution Reason | Recovered |

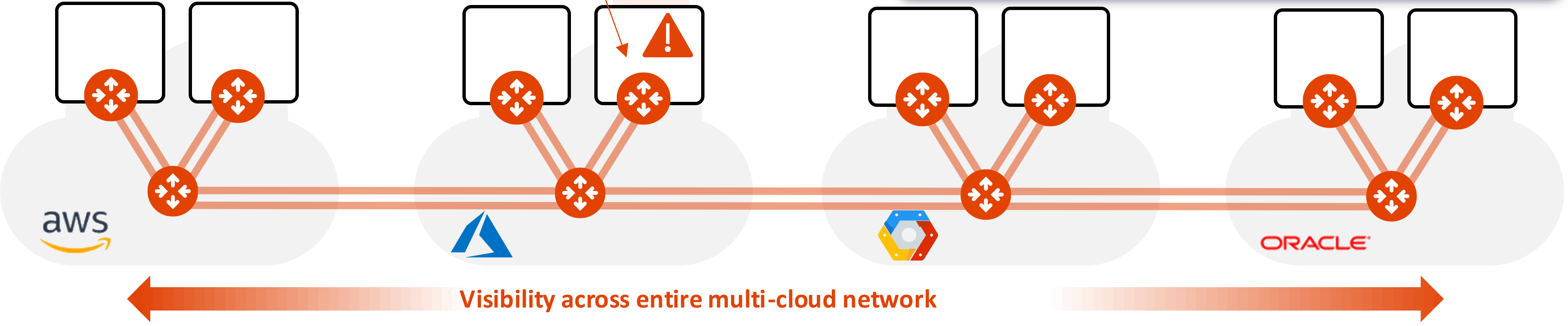


DISCOVER



| Source IP | Destina... | Port | Protocol | Description | Action |
|---|---|---|---|---|---|
| 8.218.248.168/32 | 0.0.0.0/0 | ALL | ALL | ThreatIQ 2021-11-10T17:4... | force-drop |
| 0.0.0.0/0 | 8.218.248.168/32 | ALL | ALL | ThreatIQ 2021-11-10T17:4... | force-drop |

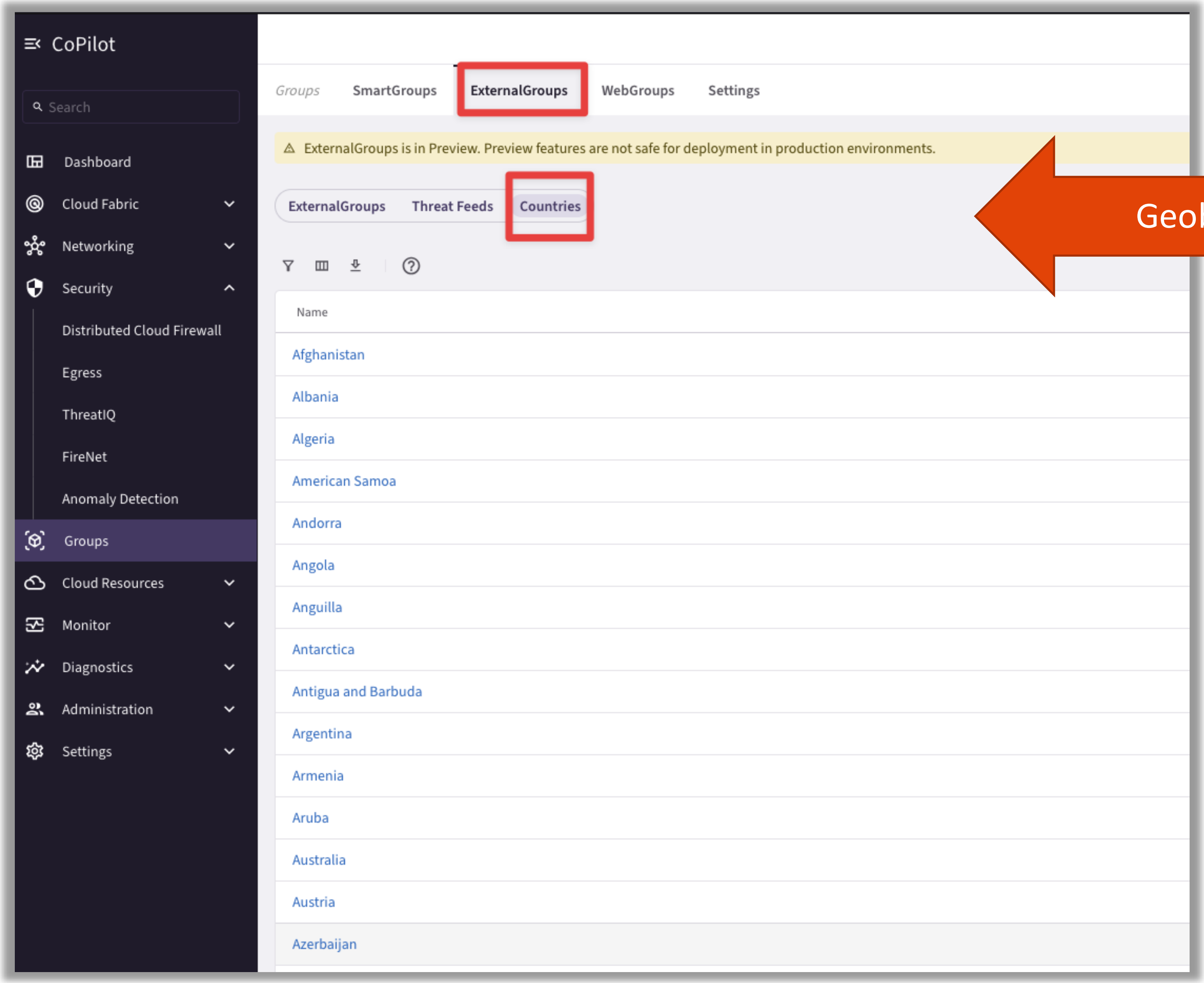
Firewall Rules



Visibility across entire multi-cloud network

AVIATRIX
ACE
SECURITY
SPECIALTY

# Block Threats Based on Geographic Location



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

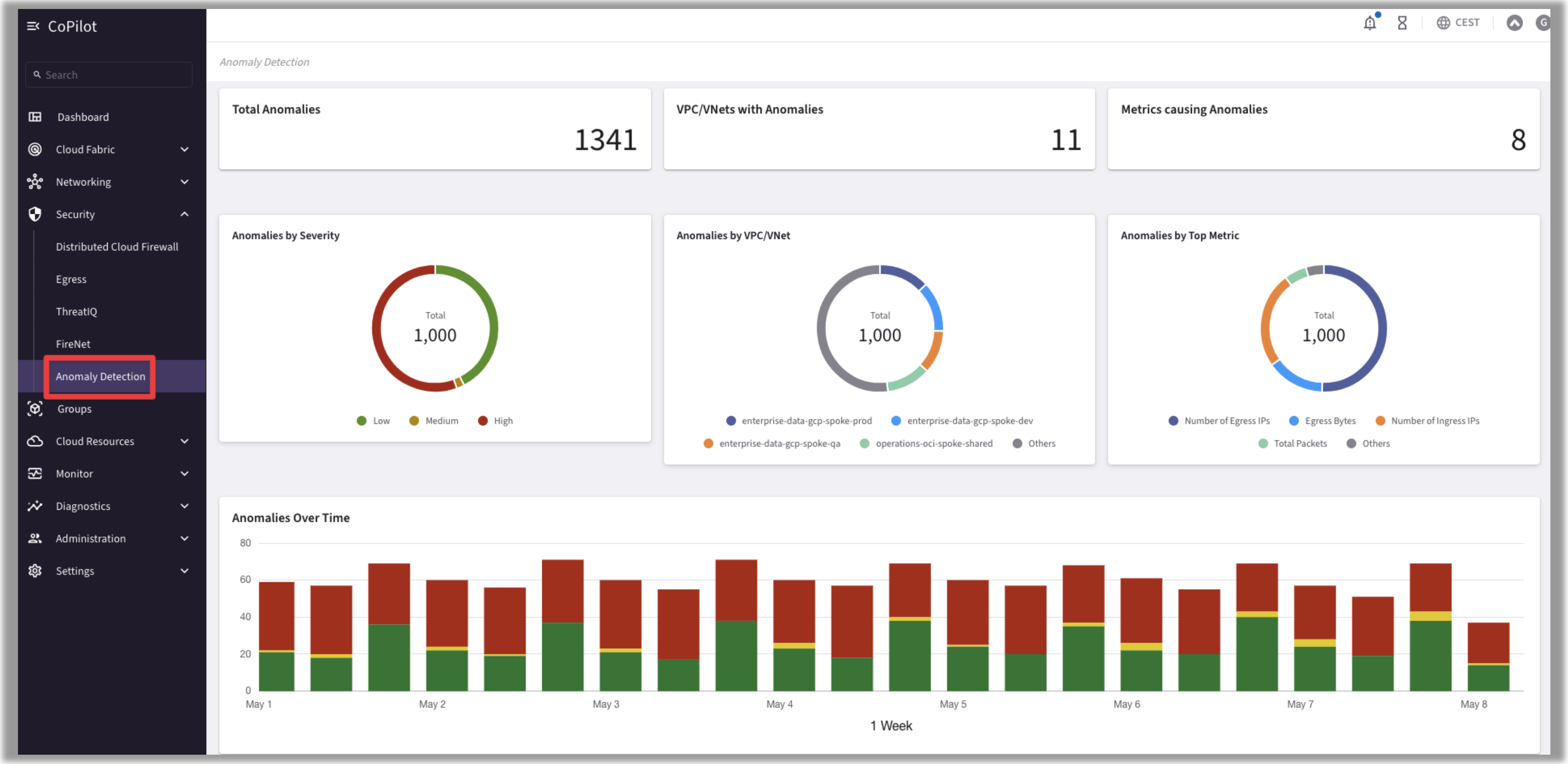
| Name |
|---|
| Afghanistan |
| Albania |
| Algeria |
| American Samoa |
| Andorra |
| Angola |
| Anguilla |
| Antarctica |
| Antigua and Barbuda |
| Argentina |
| Armenia |
| Aruba |
| Australia |
| Austria |
| Azerbaijan |

Geoblocking

AVIATRIX
ACE
SECURITY
SPECIALTY

# Network Behavior Analytics

## Aviatrix Anomaly Detection


CoPilot
Search
Dashboard
Cloud Fabric
Networking
Security
Distributed Cloud Firewall
Egress
ThreatIQ
FireNet
Anomaly Detection
Groups
Cloud Resources
Monitor
Diagnostics
Administration
Settings
CEST
Anomaly Detection
Total Anomalies
1341
VPC/VNets with Anomalies
11
Metrics causing Anomalies
8
Anomalies by Severity
Total
1,000
Low
Medium
High
Anomalies by VPC/VNet
Total
1,000
enterprise-data-gcp-spoke-prod
enterprise-data-gcp-spoke-dev
enterprise-data-gcp-spoke-qa
operations-oci-spoke-shared
Others
Anomalies by Top Metric
Total
1,000
Number of Egress IPs
Egress Bytes
Number of Ingress IPs
Total Packets
Others
Anomalies Over Time
80
60
40
20
0
May 1
May 2
May 3
May 4
May 5
May 6
May 7
May 8
1 Week

AVIATRIX

ACE

SECURITY

SPECIALTY

# Next: Security and Operational Visibility