Security Close to the Applications

THREATIQ, GEOBLOCKING AND ANOMALY DETECTION
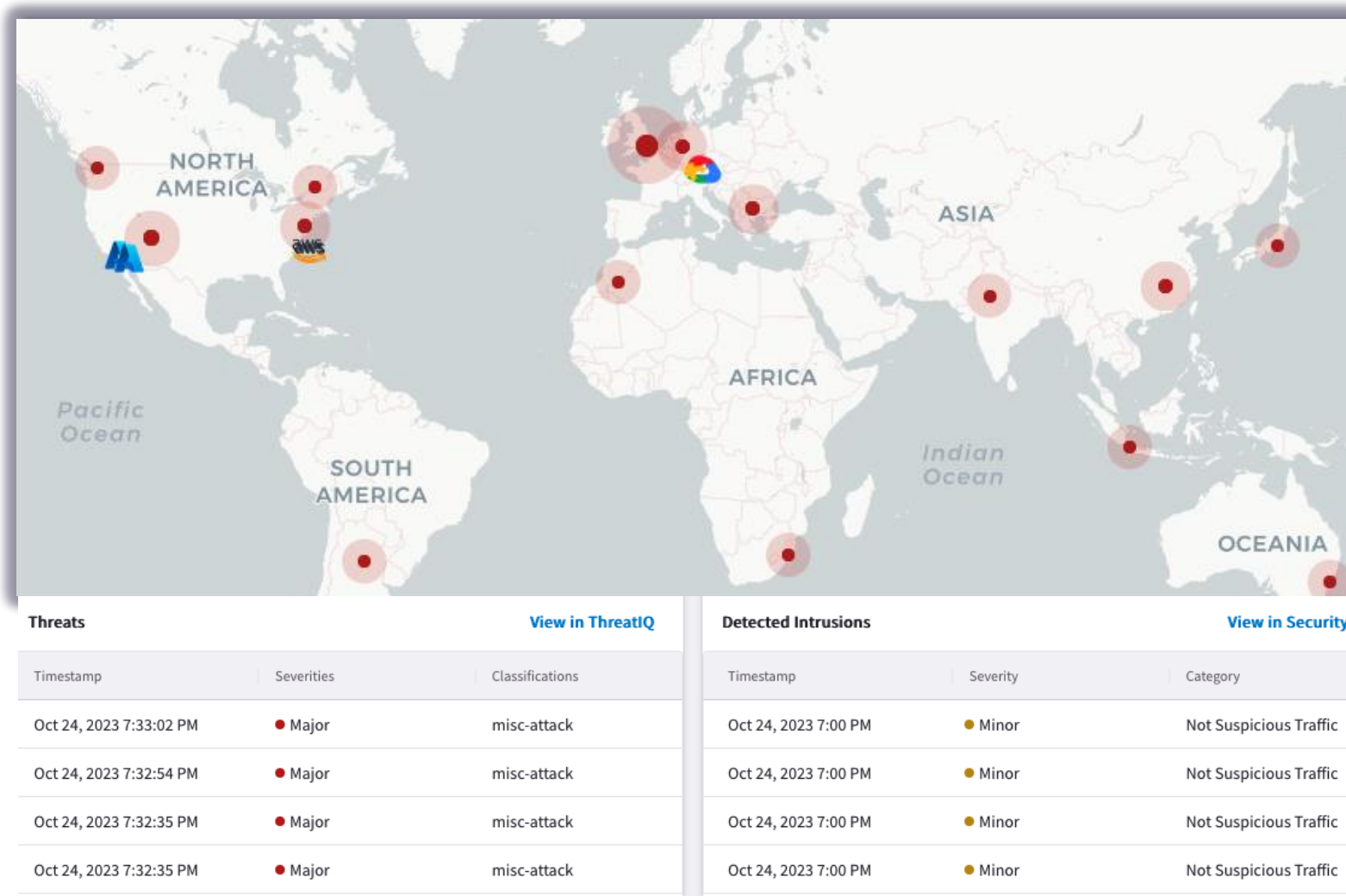
What is it?

- 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

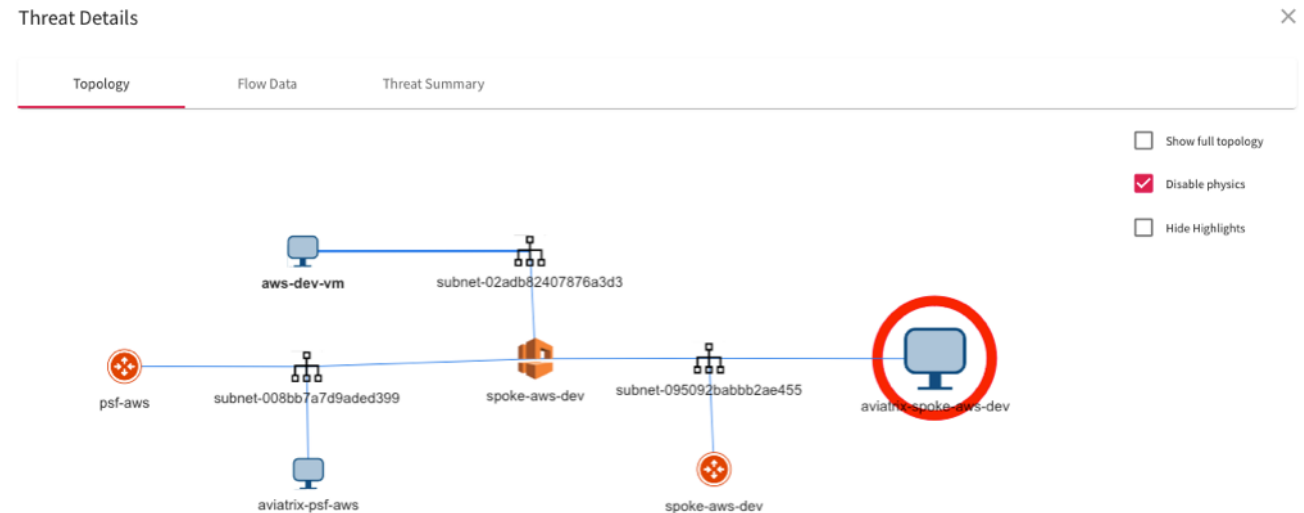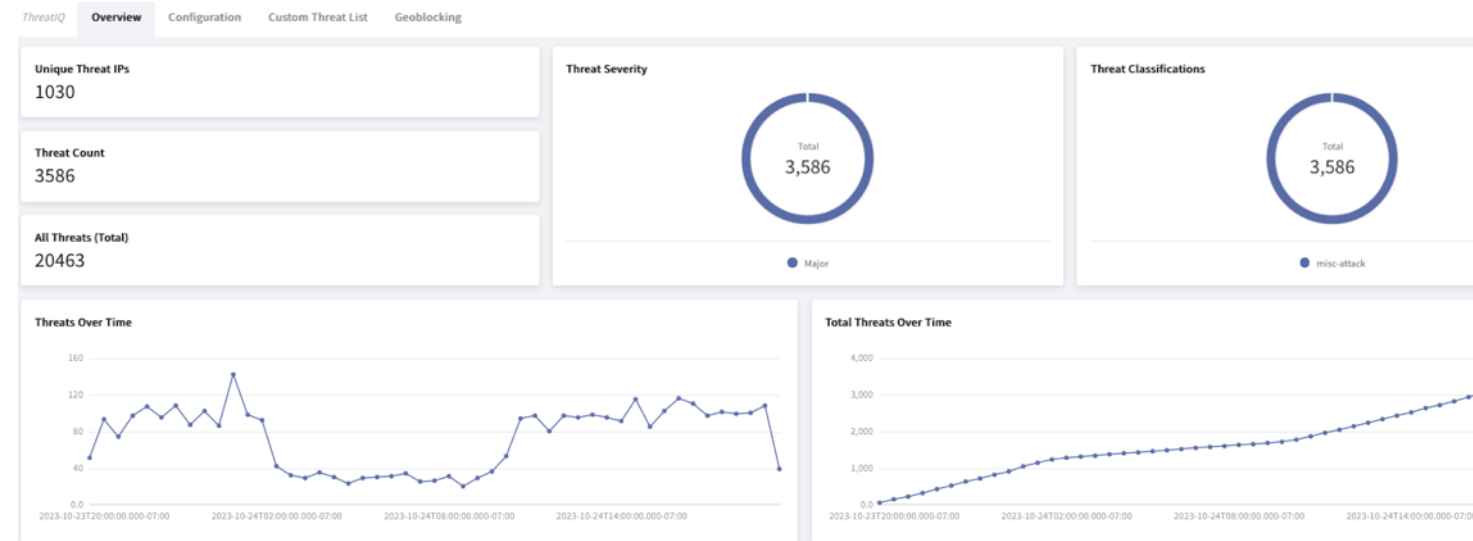Workloads   Workloads
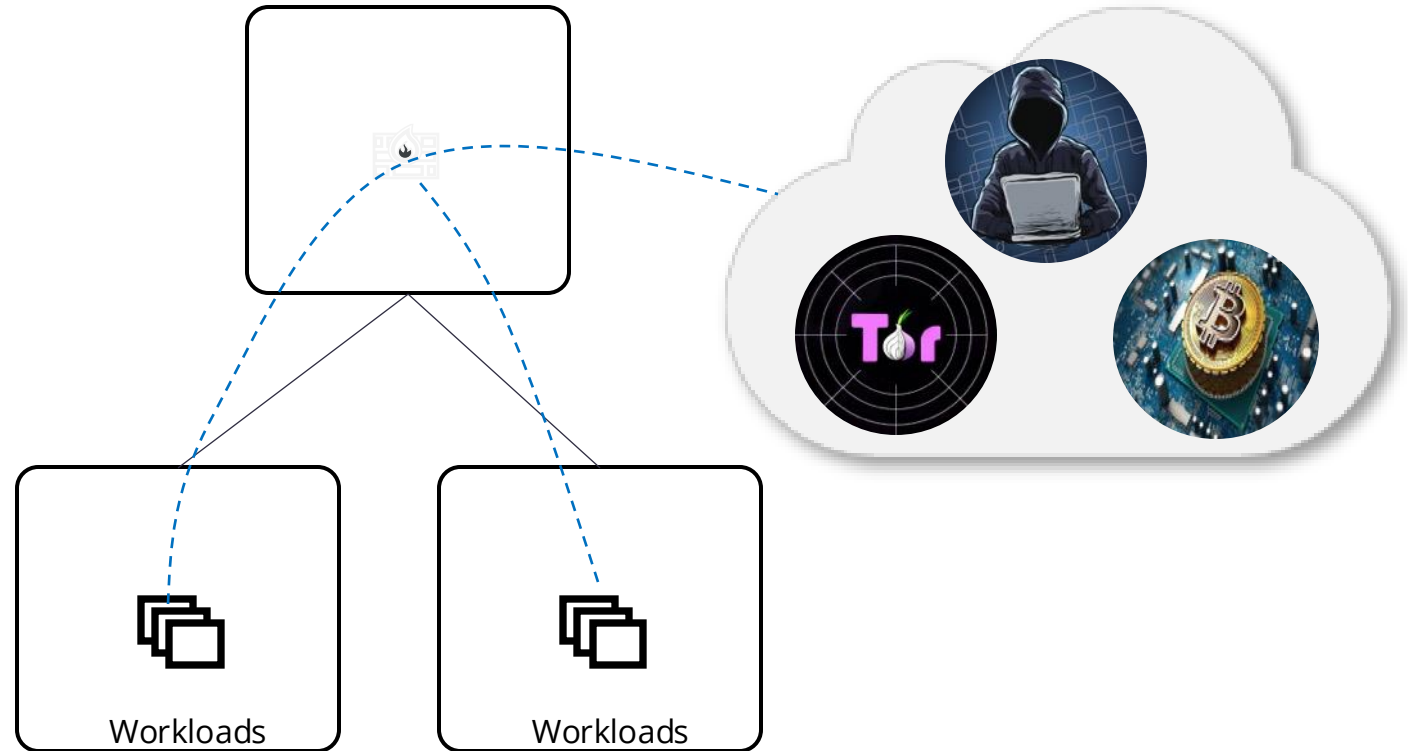
How does it work?

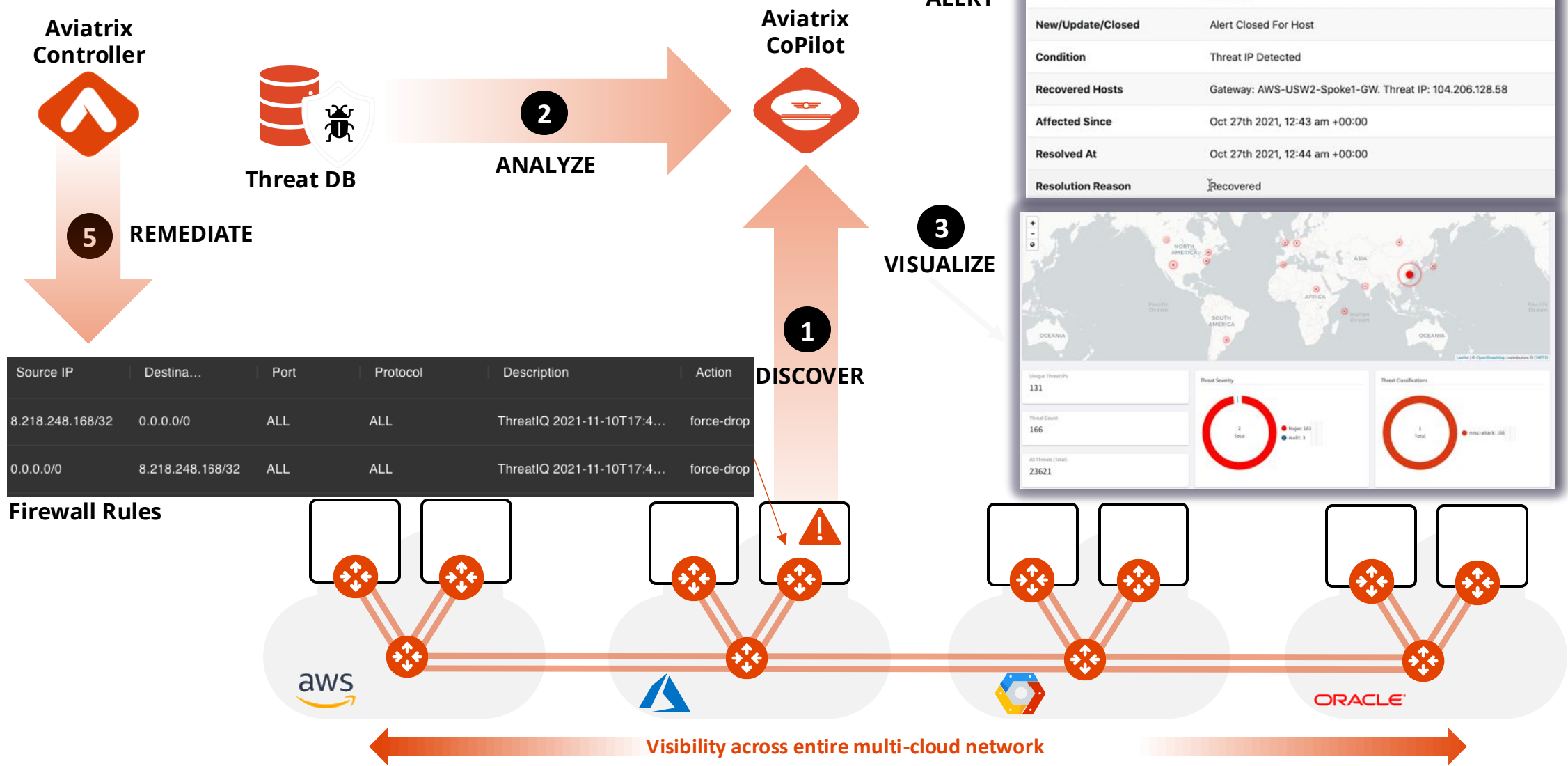- **Distributed Inspection & Notification**

  - 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

Workflow

Aviatrix Controller

Threat DB

Aviatrix CoPilot

2 ANALYZE

5 REMEDIATE

1 DISCOVER

3 VISUALIZE

4 ALERT

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

Unique Threat IPs: 131
Threat Count: 166
All Threats (Total): 23621

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

aws

ORACLE

Visibility across entire multi-cloud network

aviatrix®

Block Threats Based on Geographic Location

Network Behavior Analytics

Aviatrix Anomaly Detection

Dashboard

Cloud Fabric

Networking

Security
- Distributed Cloud Firewall
- Egress
- ThreatIQ

Anomaly Detection

Cloud Resources

Monitor

Diagnostics

Billing & Cost

Administration

Settings

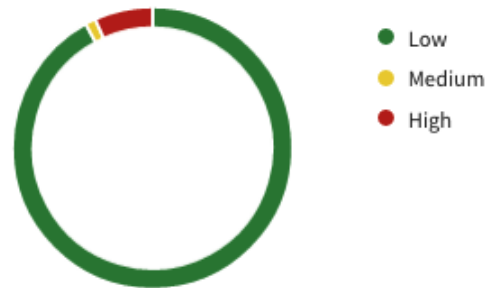**▲ aviatrix**

Total Anomalies

1634

VPC/VNets with Anomalies

5

Metrics causing Anomalies

8

Anomalies by Severity

- ● Low
- ● Medium
- ● High

Anomalies by VPC/VNet

- ● accounting-aws-spok...
- ● engineering-aws-spok...
- ● marketing-azure-spok...
- ● operations-oci-spoke-...
- ● enterprise-data-gcp-s...

Anomalies by Top Metric

- ● Number of Egress Ports
- ● Number of Ingress Ports
- ● Egress Bytes
- ● Total Packets
- ● Total Bytes
- ● Number of Ingress IPs
- ● Ingress Bytes

Anomalies Over Time

100

50

0

Sep 25 Sep 26 Sep 27 Sep 28 Sep 29 Sep 30 Oct 1 Oct 2 Oct 3 Oct 4 Oct 5 Oct 6 Oct 7 Oct 8 Oct 9 Oct 10 Oct 11 Oct 12 Oct 13 Oct 14 Oct 15 Oct 16 Oct 17 Oct 18 Oct 19 Oct 20 Oct 21 Oct 22 Oct 23 Oct 24

1 Month

Total Anomalies (Cumulative)

6000

4000

2000

0

Sep 25 Sep 26 Sep 27 Sep 28 Sep 29 Sep 30 Oct 1 Oct 2 Oct 3 Oct 4 Oct 5 Oct 6 Oct 7 Oct 8 Oct 9 Oct 10 Oct 11 Oct 12 Oct 13 Oct 14 Oct 15 Oct 16 Oct 17 Oct 18 Oct 19 Oct 20 Oct 21 Oct 22 Oct 23 Oct 24

1 Month
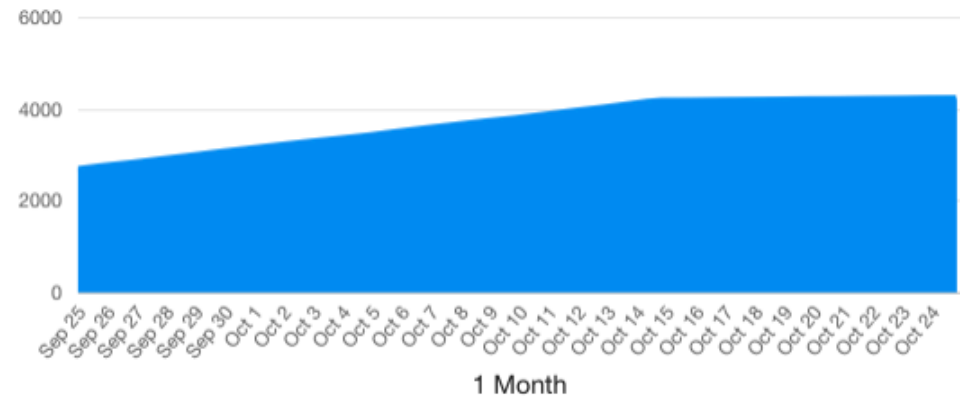
Ⅲ Columns   � Filters   ☰ Density   ⬇ Export

Search Anomalies

Detected At ↓ 1	VPC/VNet	Cloud ↑ 2	Metrics	Severity	Anomaly
Oct 8, 2023 3:00:11 PM	accounting-aws-spoke-dev	AWS	3	Low	🔵
Oct 8, 2023 3:00:11 PM	engineering-aws-spoke-dev	AWS	3	Low	🔵

Manage Monitored VPC/VNets

Available
0/2 selected

Filter

	VPC/VNet Name	Cloud	Region
☐	operations-aws-spoke-landing-z	aws	us-east-1
☐	sv-metro-equinix-demo-edge-site	aviatrix	avx-edge-default

Monitored
0/16 selected

Filter

	VPC/VNet Name	Cloud	Region
☐	accounting-aws-spoke-dev	aws	us-east-1
☐	accounting-aws-spoke-prod	aws	us-east-1
☐	accounting-aws-spoke-qa	aws	us-east-1
☐	engineering-aws-spoke-dev	aws	us-east-2
☐	engineering-aws-spoke-prod	aws	us-east-2
☐	engineering-aws-spoke-qa	aws	us-east-2
☐	enterprise-data-gcp-spoke-dev	gcp	us-west1
☐	enterprise-data-gcp-spoke-prod	gcp	us-west1
☐	enterprise-data-gcp-spoke-qa	gcp	us-west1

Learning Period

This is only set for the newly added VPC/VNets and does not change any learning period for already monitored VPC/VNets

Learning Period (Weeks)
4

Min: 2 Weeks | Max: 52 Weeks

Configu

Monitored V

16 ✏

Last Hour

Total Anoma

Anomalies by

Anomalies O

Monitored VPC/VNets

🔽 ▥ ⬇   🔍 Search

VPC/VNet	Cloud	Region	Learning	Detection
accounting-aws-spoke-dev	AWS	us-east-1	Complete	Active
accounting-aws-spoke-prod	AWS	us-east-1	Complete	Active
accounting-aws-spoke-qa	AWS	us-east-1	Complete	Active
engineering-aws-spoke-dev	AWS	us-east-2	Complete	Active
engineering-aws-spoke-prod	AWS	us-east-2	Complete	Active
engineering-aws-spoke-qa	AWS	us-east-2	Complete	Active
enterprise-data-gcp-spoke...	Gcloud	us-west1	Complete	Active
enterprise-data-gcp-spoke...	Gcloud	us-west1	Complete	Active
enterprise-data-gcp-spoke...	Gcloud	us-west1	Complete	Active
marketing-azure-spoke-all	Azure ARM	North Europe	Complete	Active
operations-oci-spoke-shared	Oracle Cloud Infrastructure	ap-singapore-1	Complete	Active
transit-aws-us-east-1	AWS	us-east-1	Complete	Active

Total 16 VPC/VNets

Close

13

Aviatrix Certified Engineer (ACE)
https://aviatrix.com/ACE

COMMUNITY
https://community.aviatrix.com