aviatrix
ACE
Aviatrix Certified
Engineer

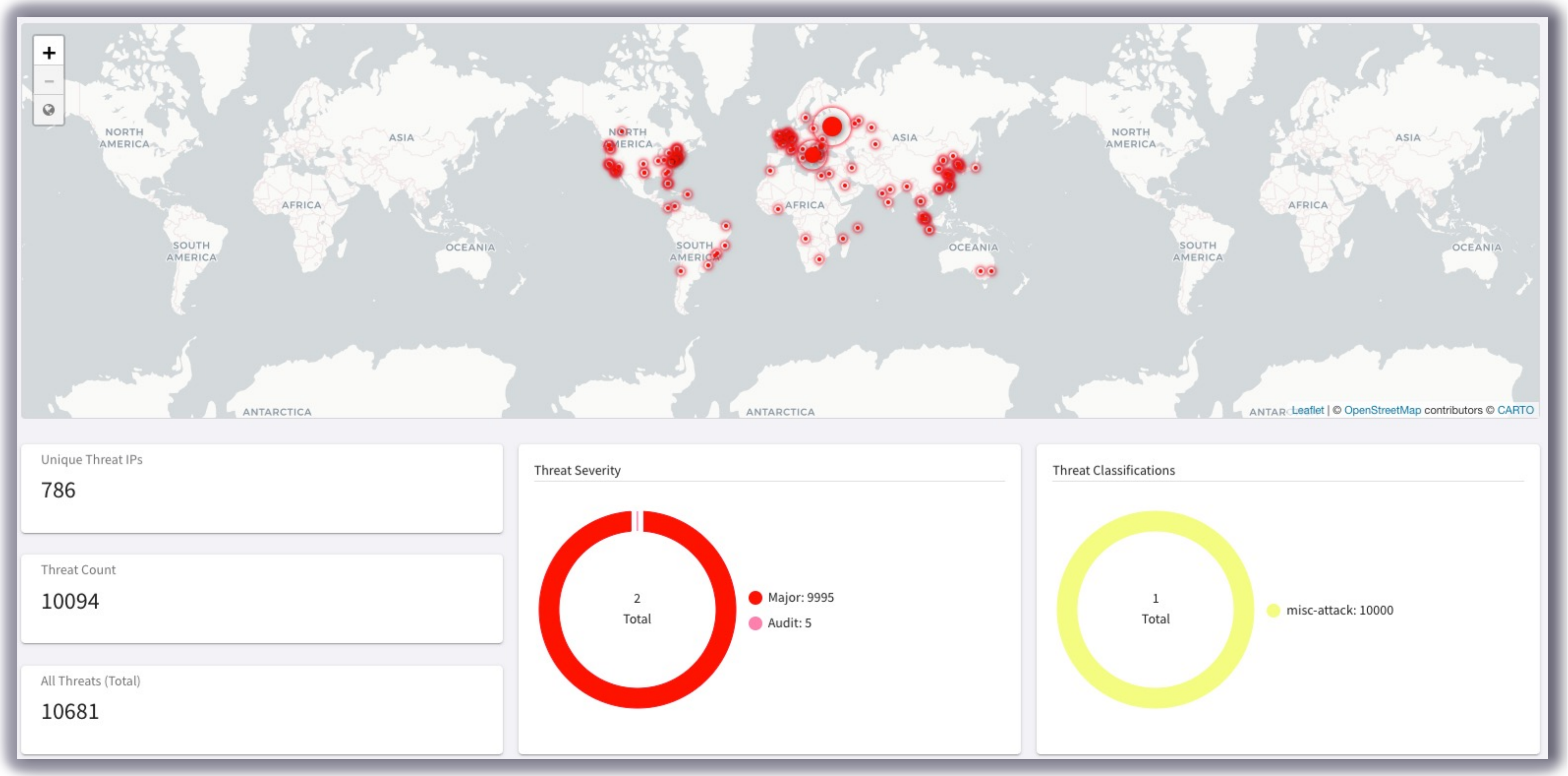
ThreatIQ

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 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


+
−
NORTH AMERICA
ASIA
AFRICA
SOUTH AMERICA
OCEANIA
ANTARCTICA
Leaflet | © OpenStreetMap contributors © CARTO
2
Total
1
Total

Unique Threat IPs
786

Threat Count
10094

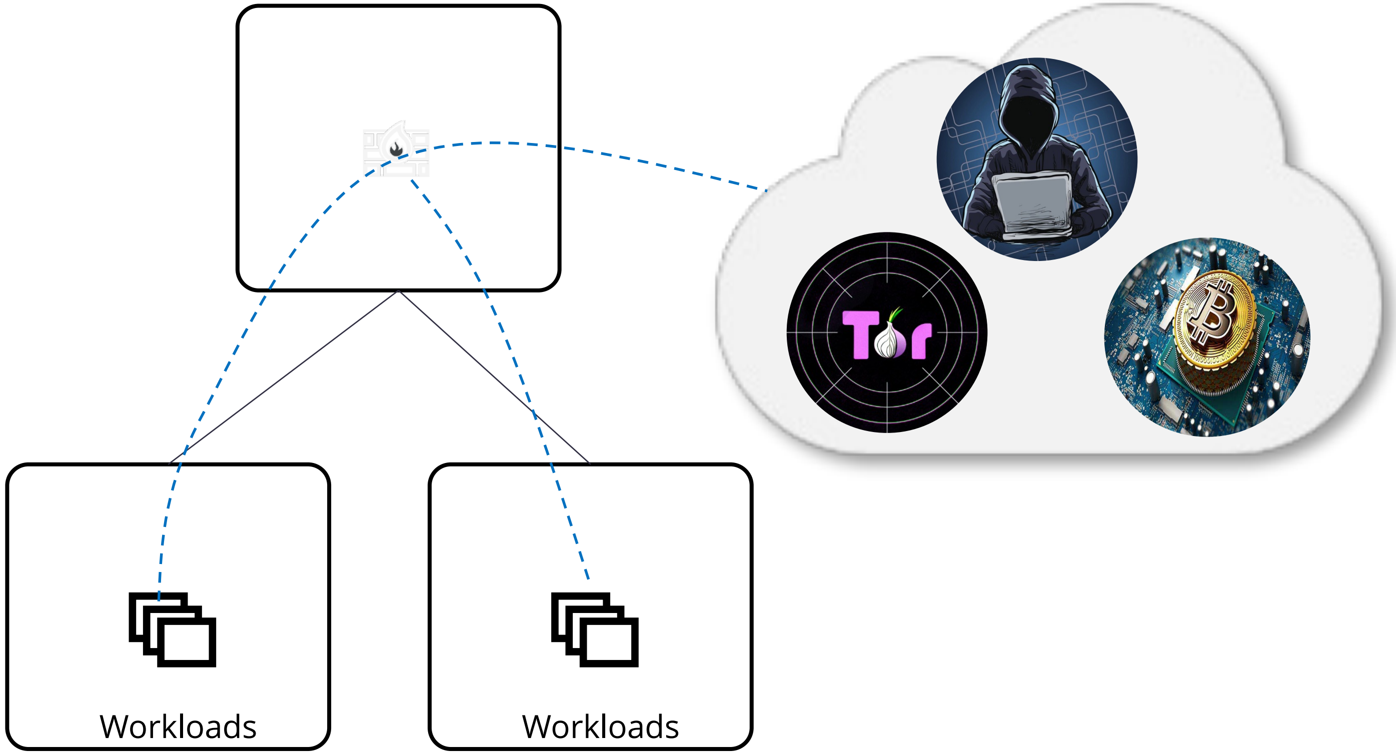
All Threats (Total)
10681

Threat Severity
- 🟥 Major: 9995
- ● Audit: 5

Threat Classifications
- ● misc-attack: 10000

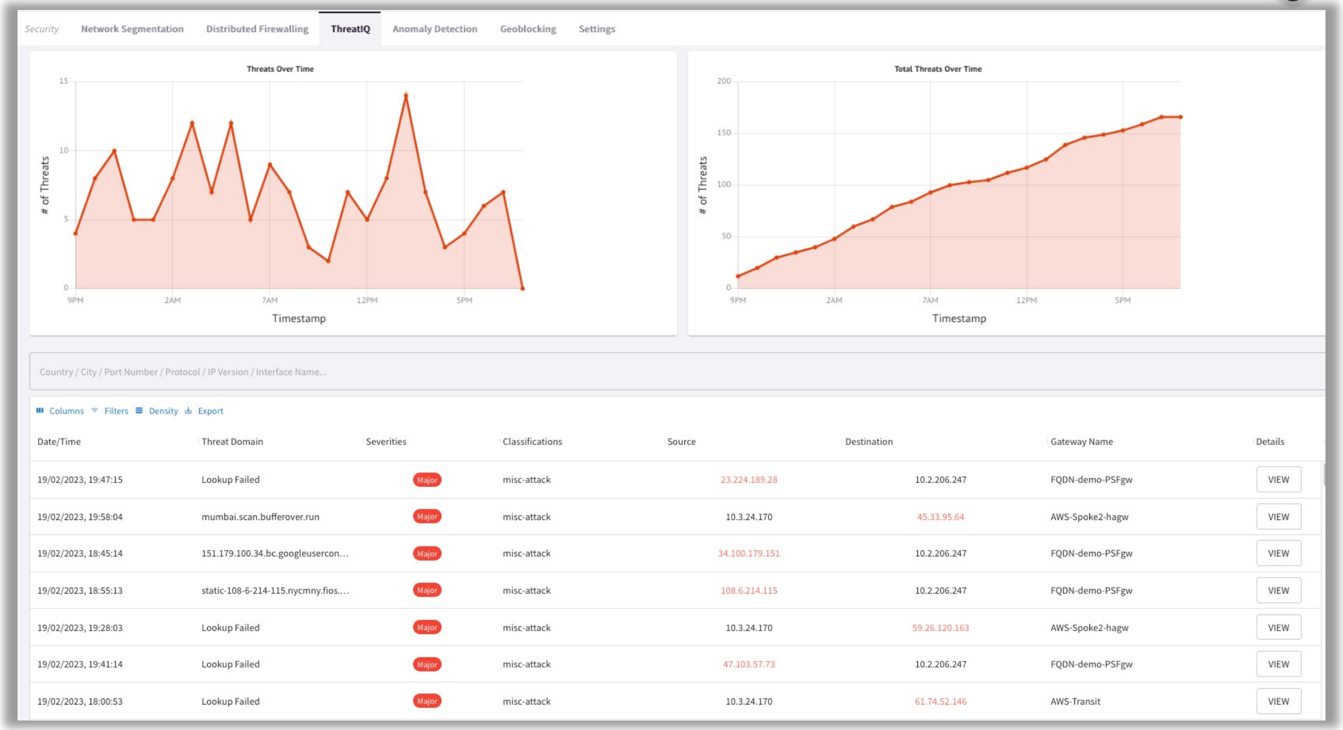
Why should enterprises care about it?

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

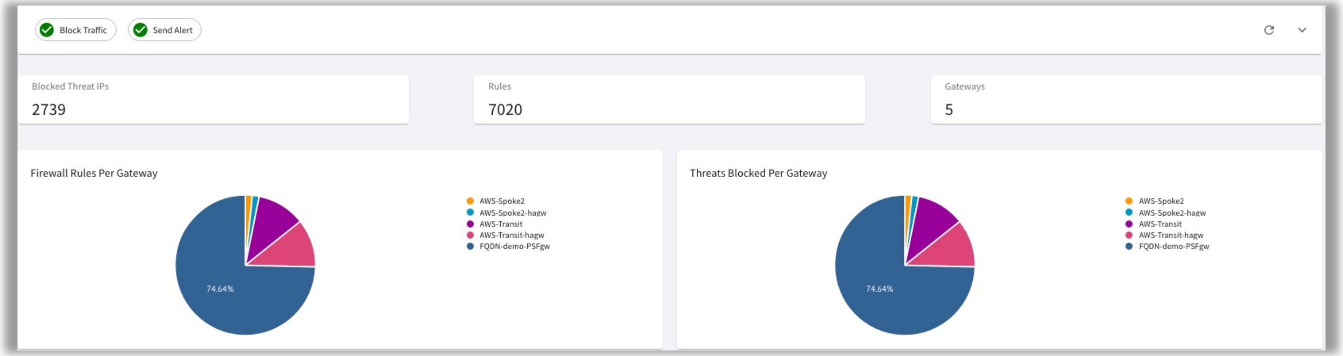


How does it work?

- **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


Security
Network Segmentation
Distributed Firewalling
ThreatIQ
Anomaly Detection
Geoblocking
Settings
Threats Over Time
15
10
5
0
# of Threats
9PM
2AM
7AM
12PM
5PM
Timestamp
Total Threats Over Time
200
150
100
50
0
# of Threats
9PM
2AM
7AM
12PM
5PM
Timestamp
Country / City / Port Number / Protocol / IP Version / Interface Name...
Columns
Filters
Density
Export

Date/Time	Threat Domain	Severities	Classifications	Source	Destination	Gateway Name	Details
19/02/2023, 19:47:15	Lookup Failed	Major	misc-attack	23.224.189.28	10.2.206.247	FQDN-demo-PSFgw	VIEW
19/02/2023, 19:58:04	mumbai.scan.bufferover.run	Major	misc-attack	10.3.24.170	45.33.95.64	AWS-Spoke2-hagw	VIEW
19/02/2023, 18:45:14	151.179.100.34.bc.googleusercon...	Major	misc-attack	34.100.179.151	10.2.206.247	FQDN-demo-PSFgw	VIEW
19/02/2023, 18:55:13	static-108-6-214-115.nycmny.fios....	Major	misc-attack	108.6.214.115	10.2.206.247	FQDN-demo-PSFgw	VIEW
19/02/2023, 19:28:03	Lookup Failed	Major	misc-attack	10.3.24.170	59.26.120.163	AWS-Spoke2-hagw	VIEW
19/02/2023, 19:41:14	Lookup Failed	Major	misc-attack	47.103.57.73	10.2.206.247	FQDN-demo-PSFgw	VIEW
19/02/2023, 18:00:53	Lookup Failed	Major	misc-attack	10.3.24.170	61.74.52.146	AWS-Transit	VIEW

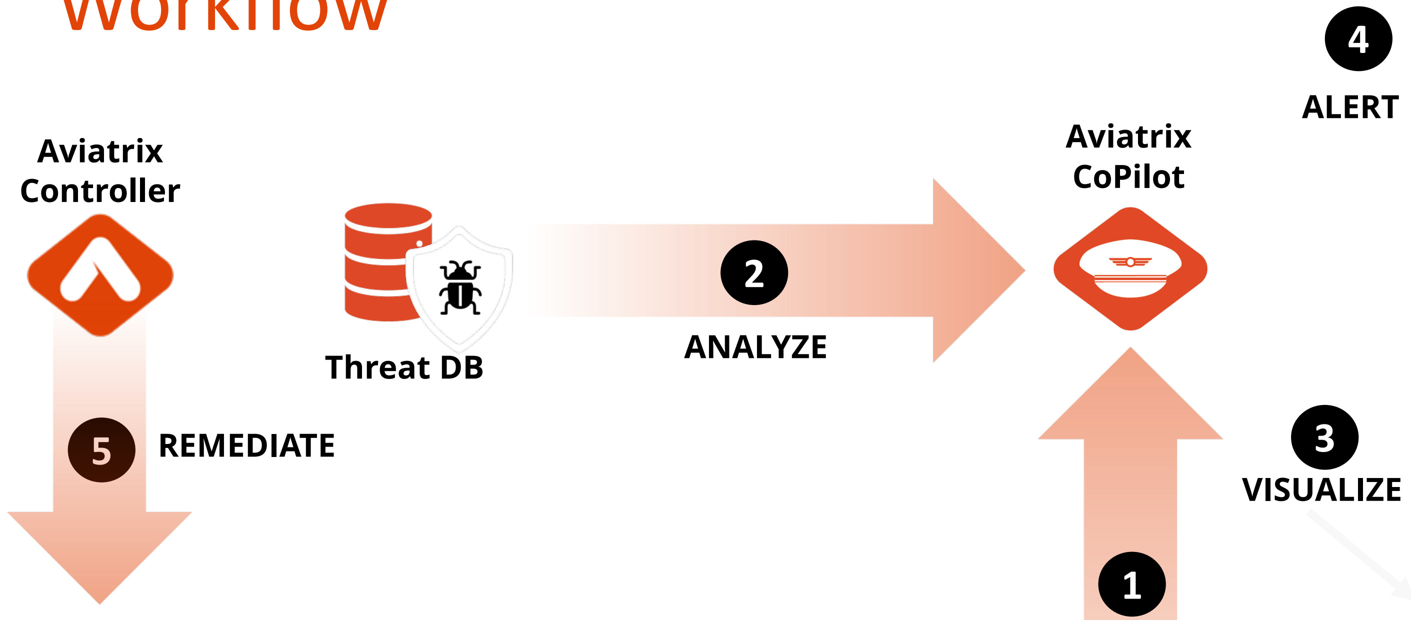

✓ Block Traffic
✓ Send Alert
Firewall Rules Per Gateway
74.64%
● AWS-Spoke2
● AWS-Spoke2-hagw
● AWS-Transit
● AWS-Transit-hagw
● FQDN-demo-PSFgw
Threats Blocked Per Gateway
74.64%
● AWS-Spoke2
● AWS-Spoke2-hagw
● AWS-Transit
● AWS-Transit-hagw
● FQDN-demo-PSFgw

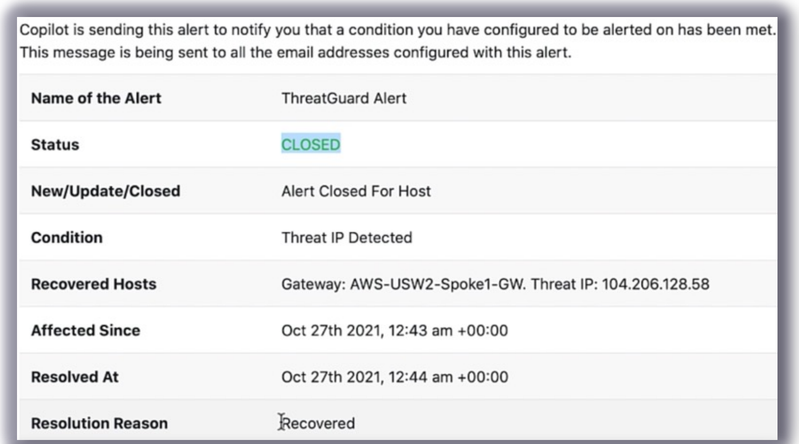
Blocked Threat IPs: 2739

Rules: 7020

Gateways: 5

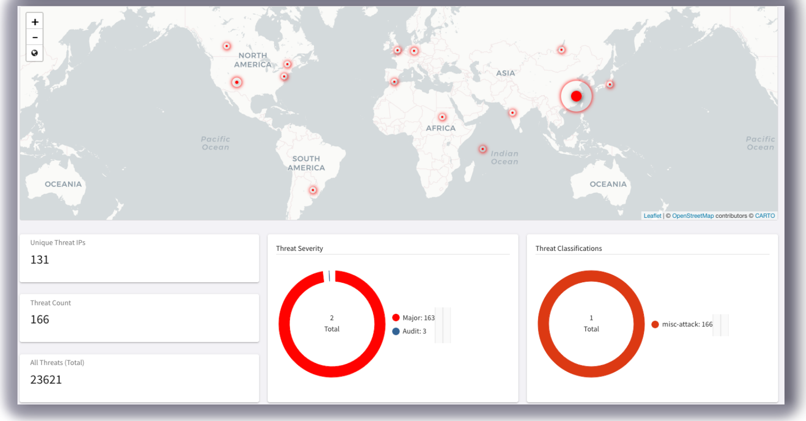
Workflow


Aviatrix Controller
Threat DB
2
ANALYZE
Aviatrix CoPilot
4
ALERT
3
VISUALIZE
5
REMEDIATE



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


NORTH AMERICA
ASIA
AFRICA
SOUTH AMERICA
OCEANIA
Pacific Ocean
Indian Ocean
Leaflet | © OpenStreetMap contributors © CARTO

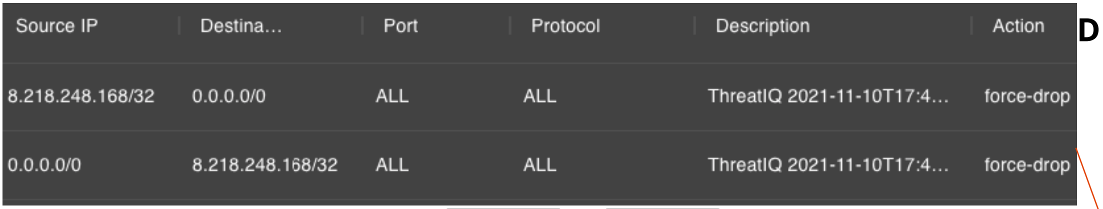
Unique Threat IPs
131

Threat Count
166

All Threats (Total)
23621

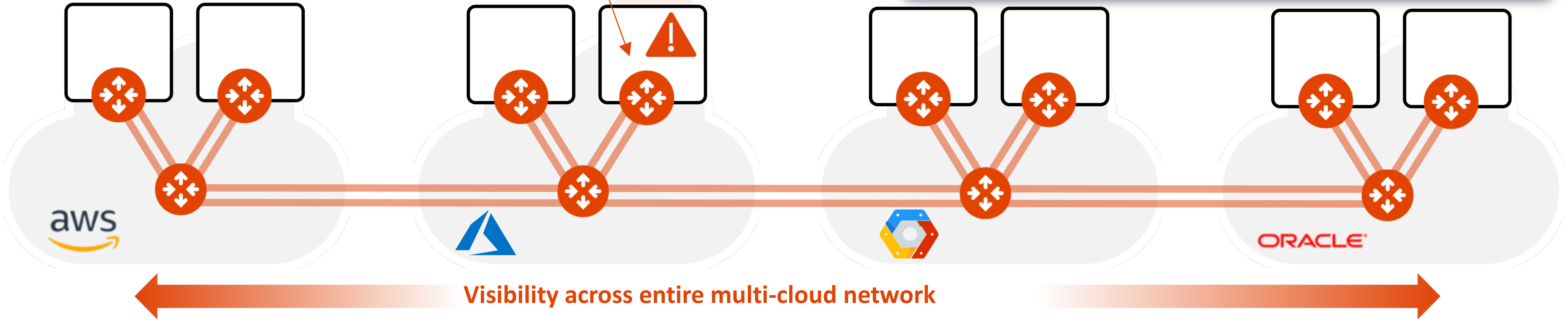
Threat Severity
2 Total
Major: 163
Audit: 3

Threat Classifications
1 Total
misc-attack: 166



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


1
DISCOVER
aws
ORACLE
Visibility across entire multi-cloud network

aviatrix
ACE
Aviatrix Certified Engineer

Next: Lab 9 – ThreatIQ