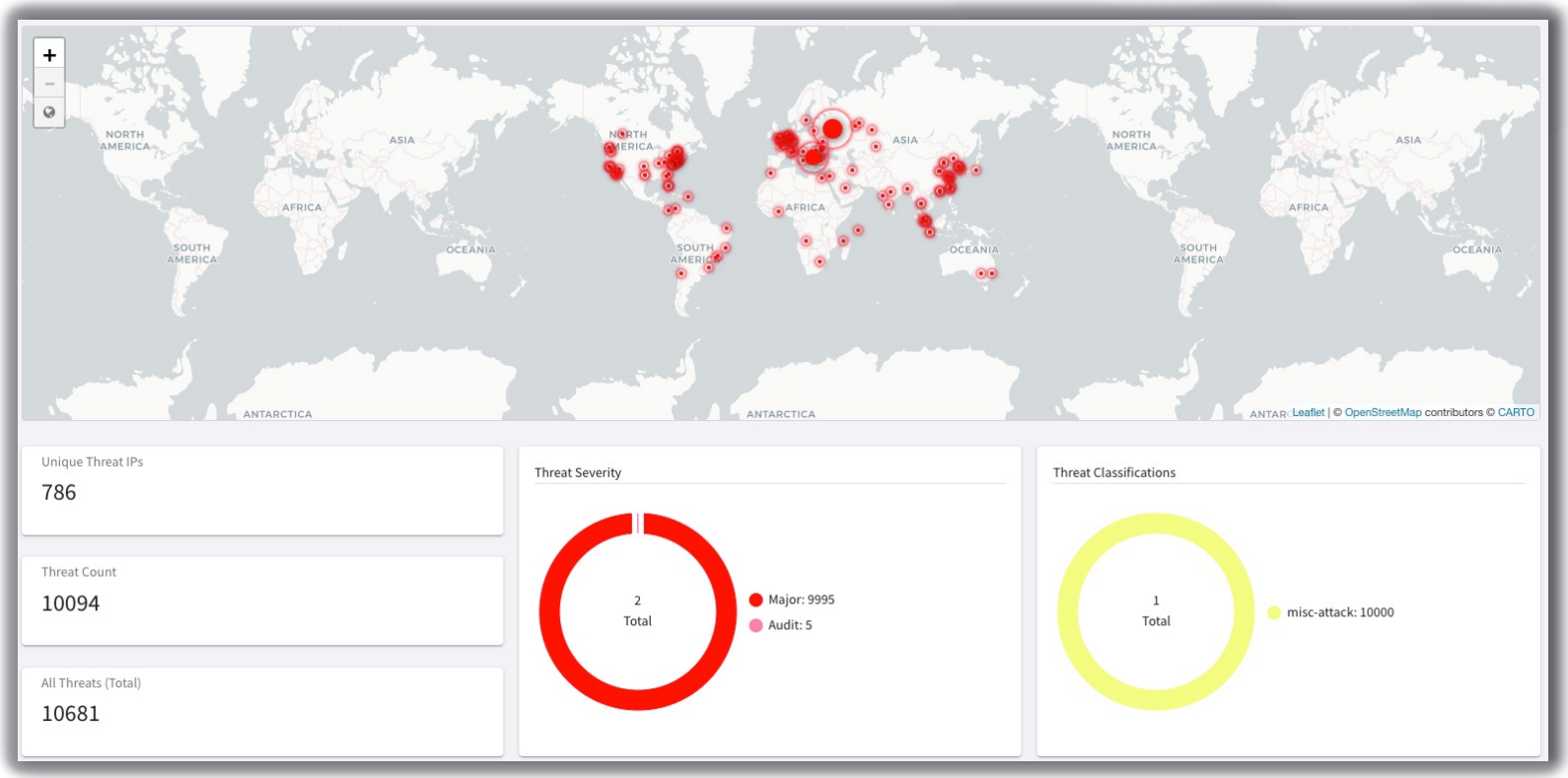
ThreatIQ

IDENTIFY AND REMEDIATE THREATS ACROSS MULTICLOUD NETWORKS

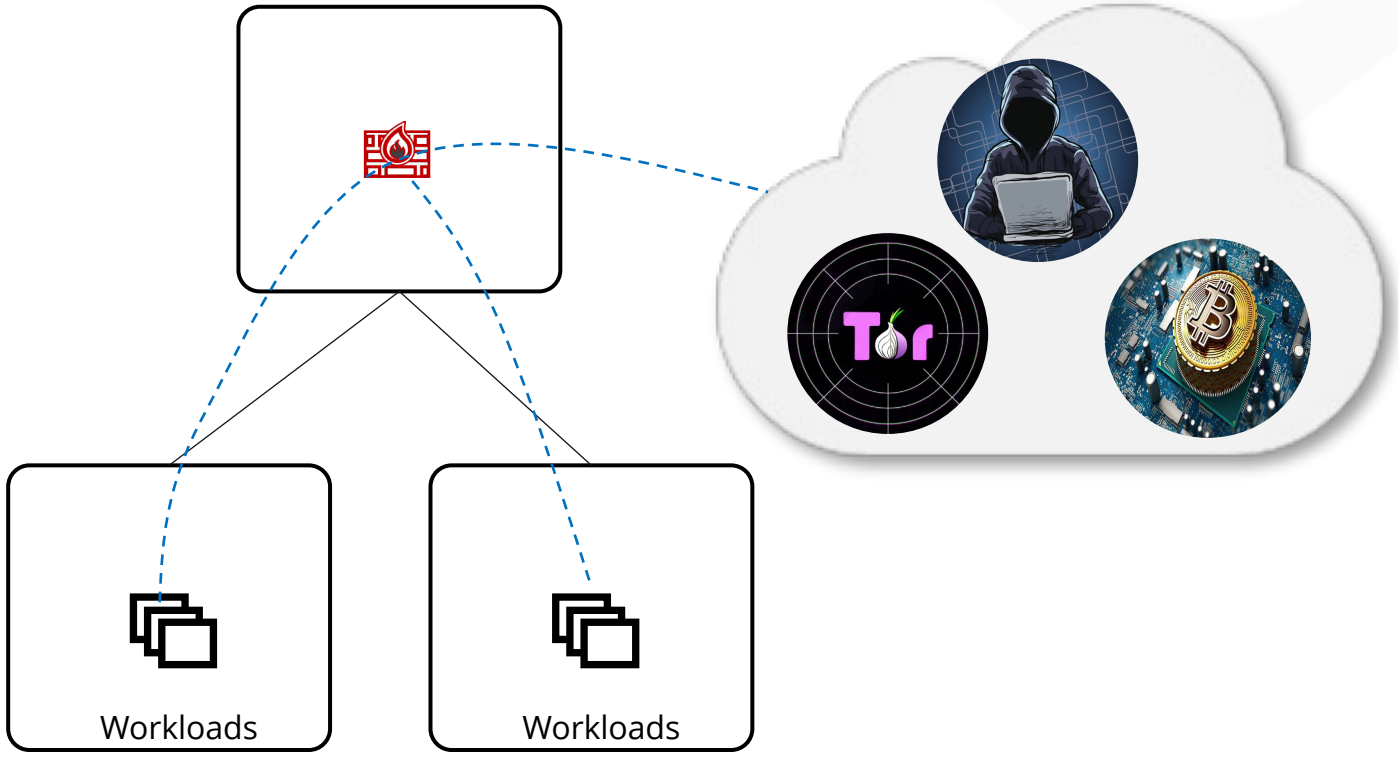
What is it?

- Multicloud native network security to dynamically **identify, alert, and remediate potential threats** to known malicious destinations
- **Distributed threat visibility** that can be enabled on all Aviatrix GWs
- Identify potential **data exfiltration and compromised host**
- **No data-plane performance impact**
- **Complementary security solution** with full multicloud support



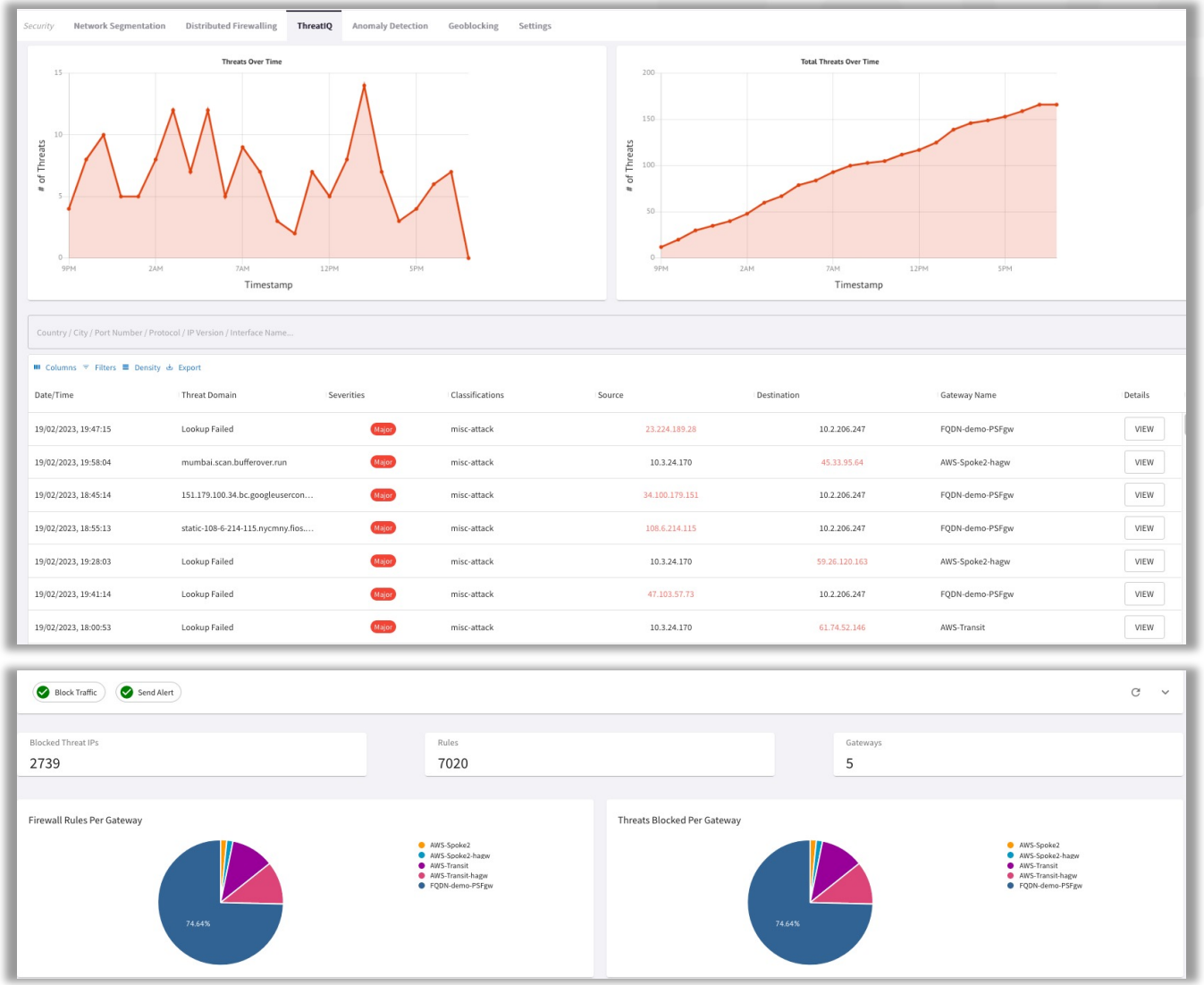
Why should enterprises care about it?

- 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



Workflow

Aviatrix Controller

Threat DB

2 ANALYZE

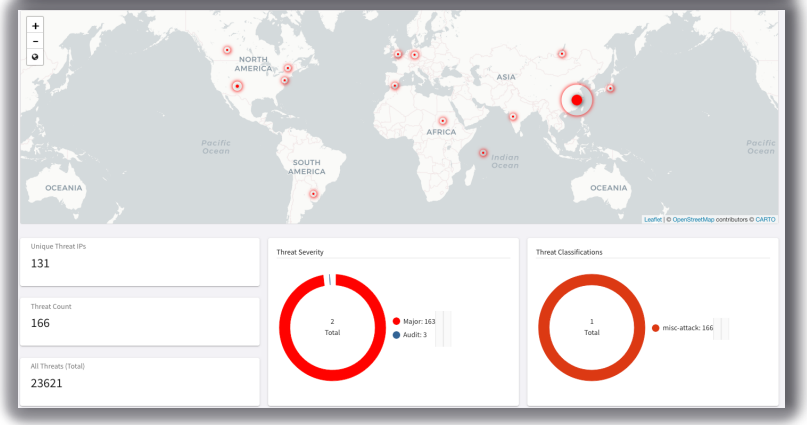
Aviatrix CoPilot

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

3 VISUALIZE

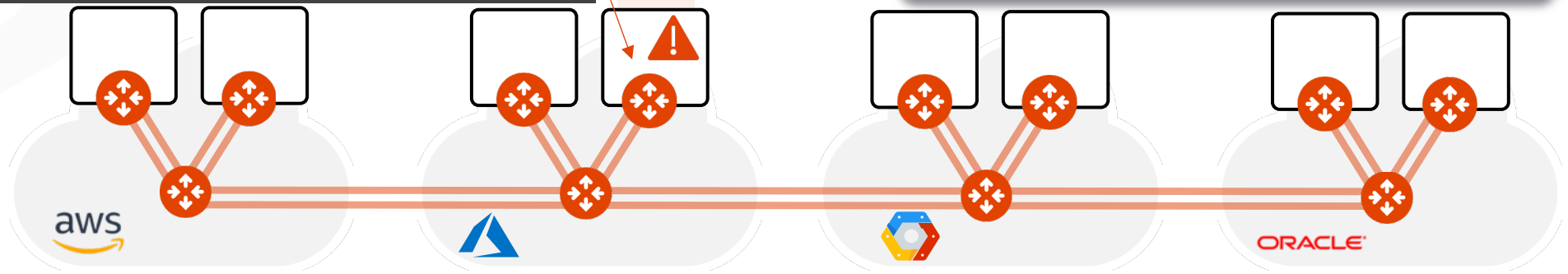


5 REMEDIATE

1 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

Next: Lab 9 – ThreatIQ and ThreatGuard