



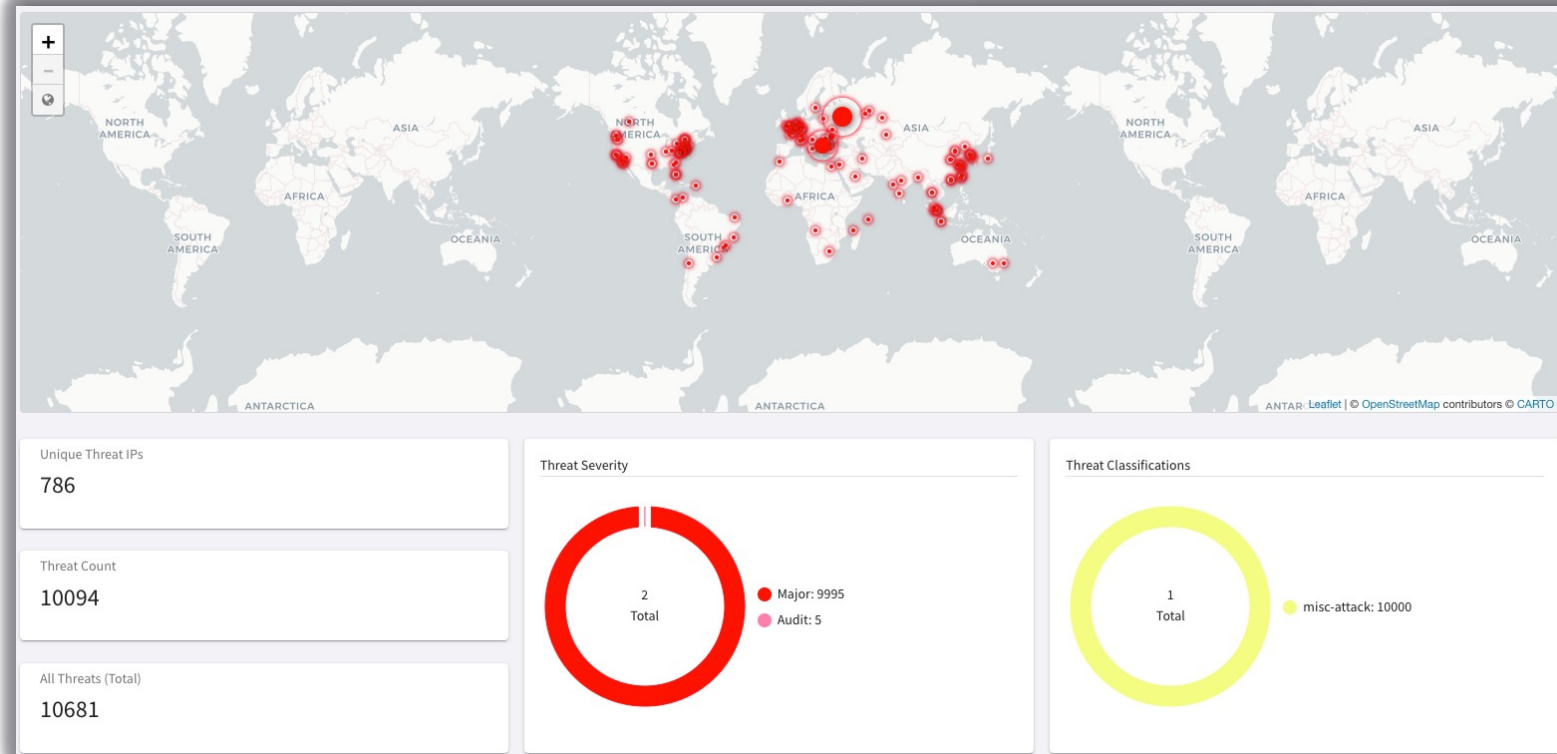
# ThreatIQ with ThreatGuard

---

IDENTIFY AND REMEDIATE THREATS ACROSS MULTICLOUD  
NETWORKS

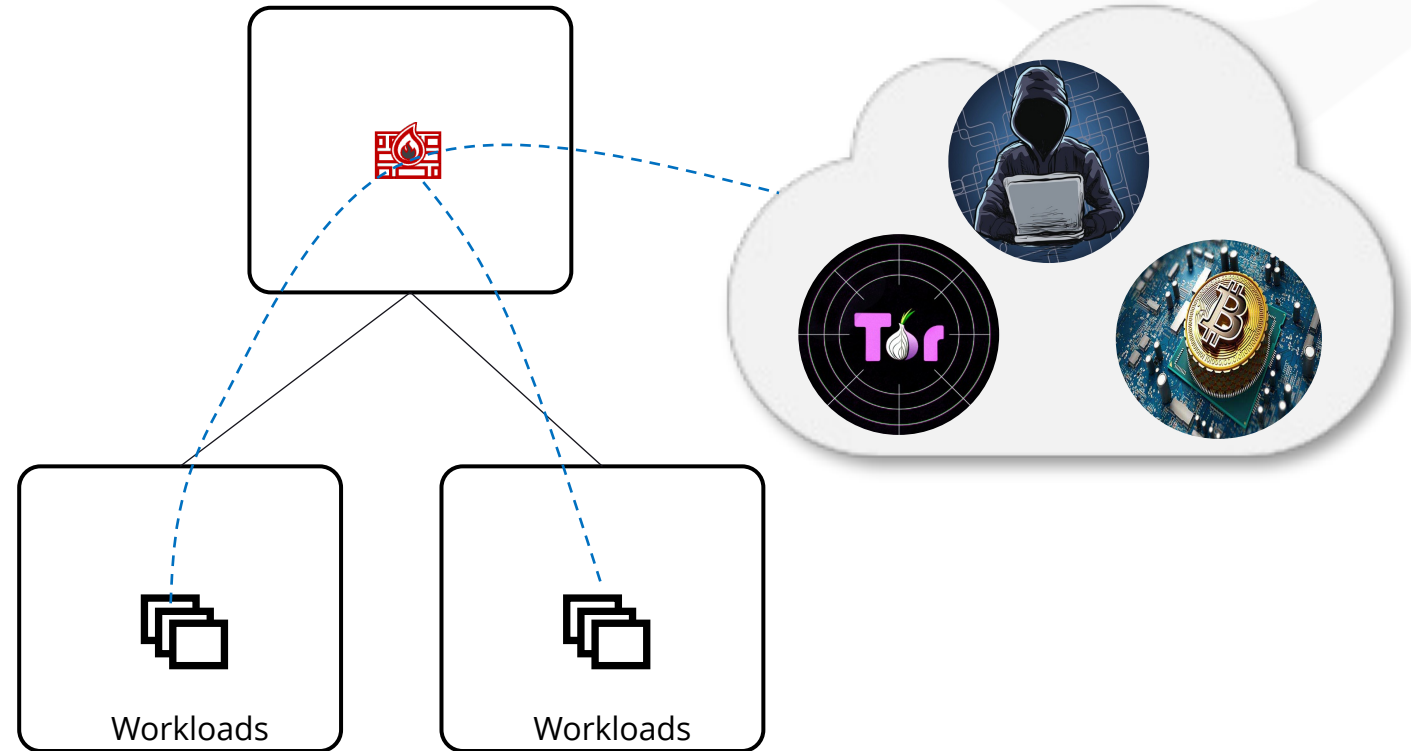
# What is it?

- Multicloud native network security to dynamically **identify, alert, and remediate potential threats** to known malicious destinations
- **Distributed threat visibility** 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



# 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



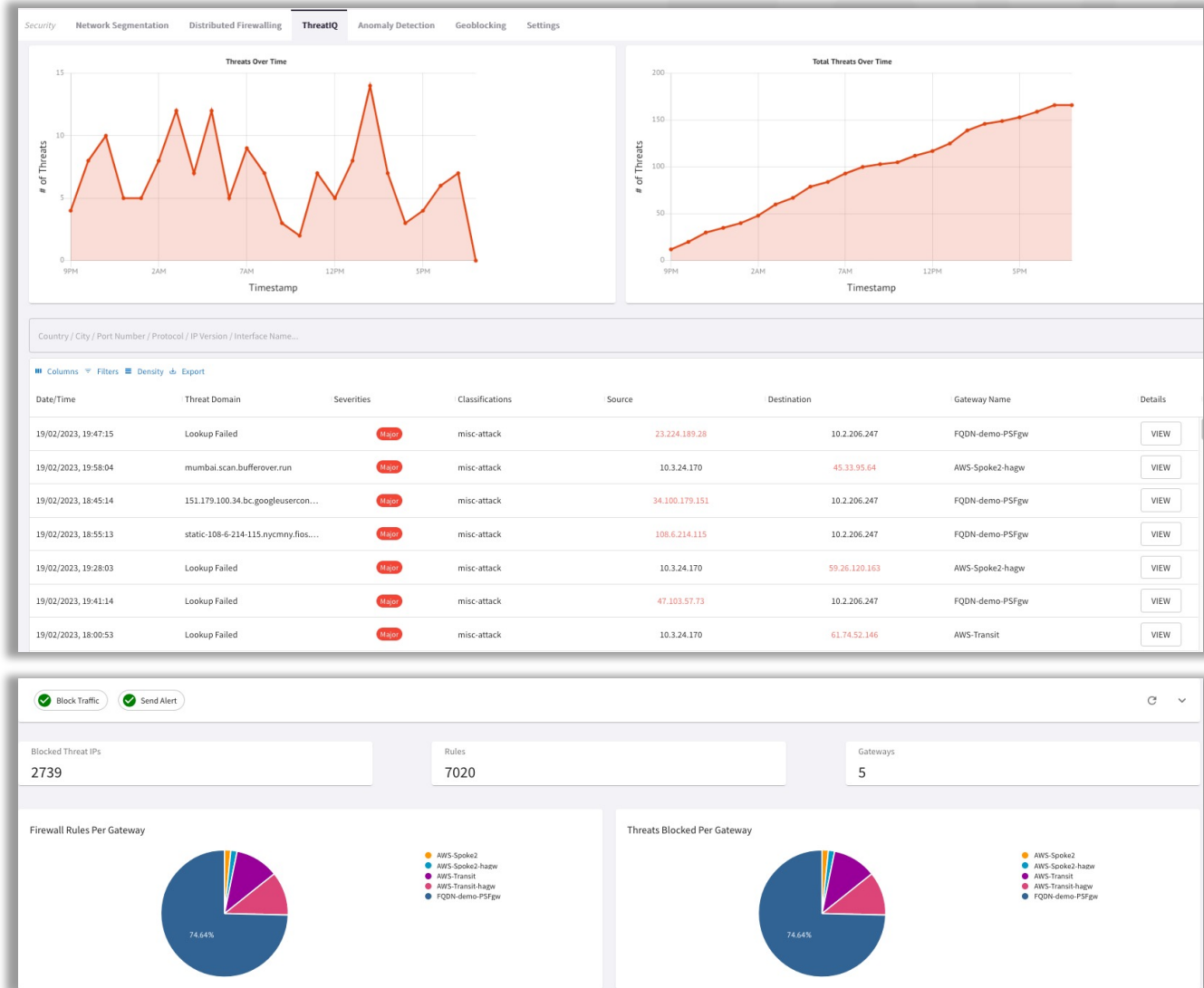
# How does it work?

## • Distributed Inspection & Notification

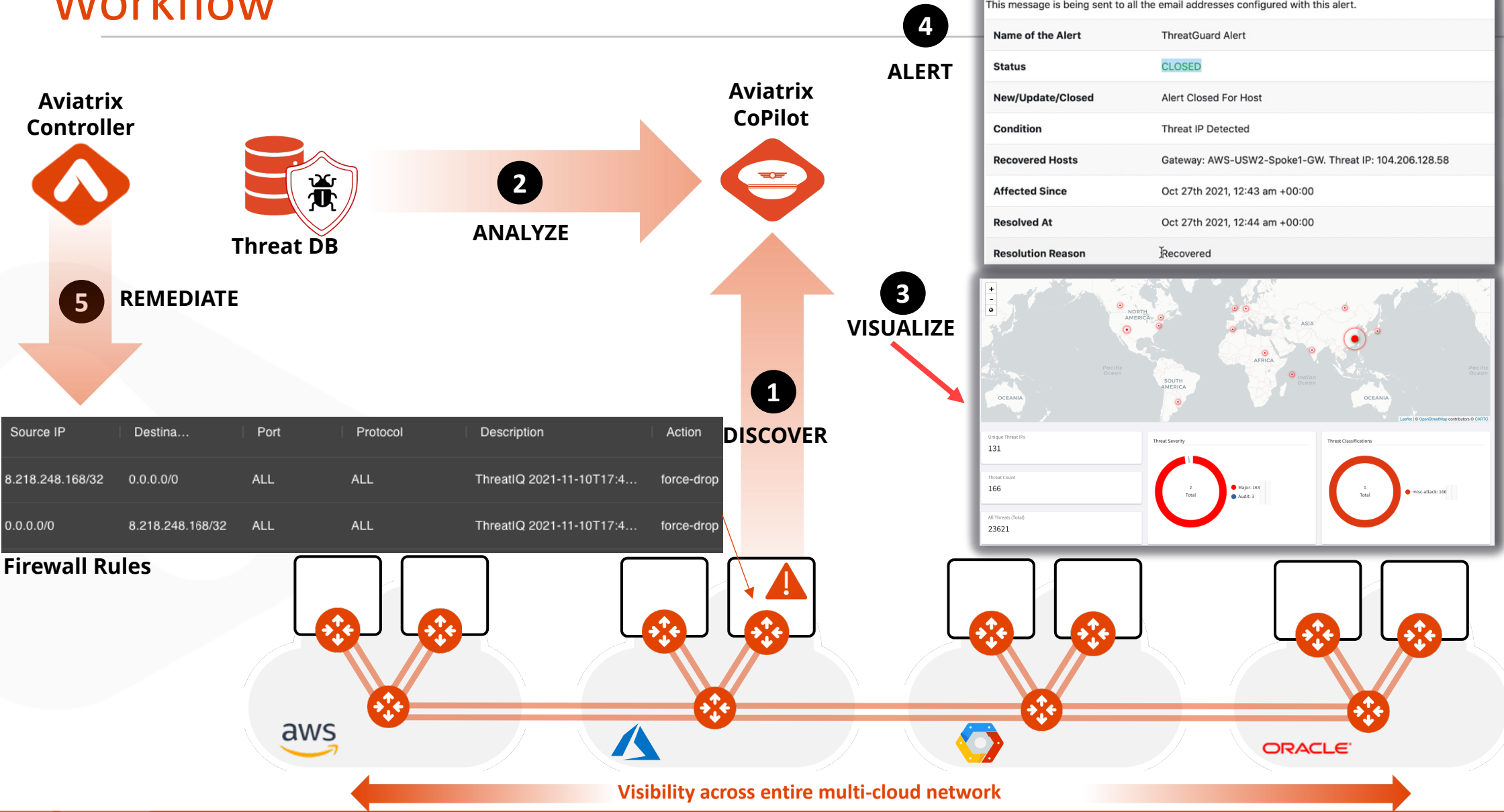
- Aviatrix gateways across Multicloud environment send real-time NetFlow data to CoPilot
- CoPilot analyzes the data on all public destinations against well-known Threat DB
- CoPilot alerts on any potential threats in the environment
- CoPilot provides extreme visibility of the impacted communication 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





Next: Lab 9 – ThreatIQ and ThreatGuard