



Security Close to the Applications

THREATIQ, GEOBLOCKING AND ANOMALY DETECTION

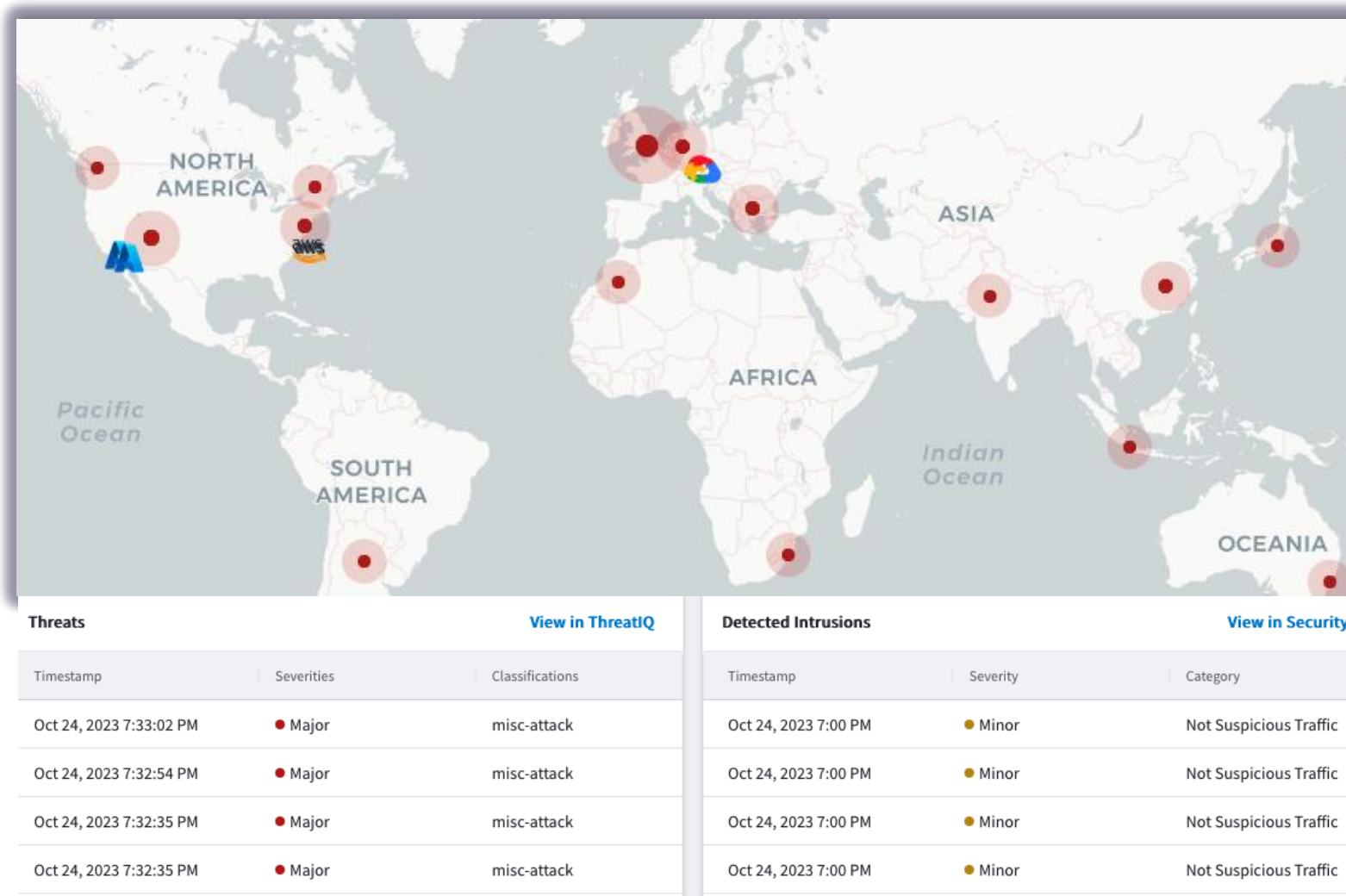


Aviatrix ThreatIQ and Threat Guard

What is it?

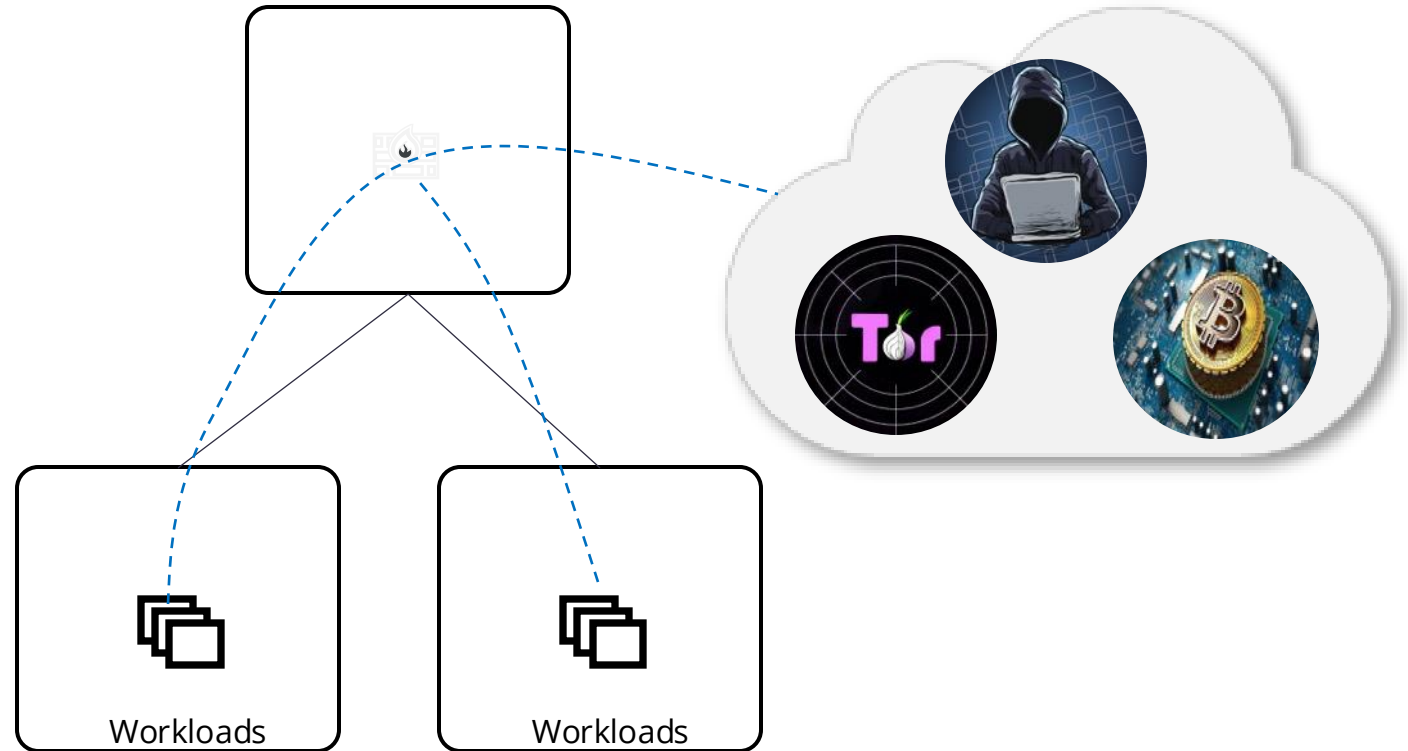


- Multicloud native network security to dynamically **identify, alert, and remediate potential threats** to known malicious destinations
- **Distributed threat visibility** and control built into the network data-plane at every hop
- Identify potential **data exfiltration and compromised host**
- **No 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?

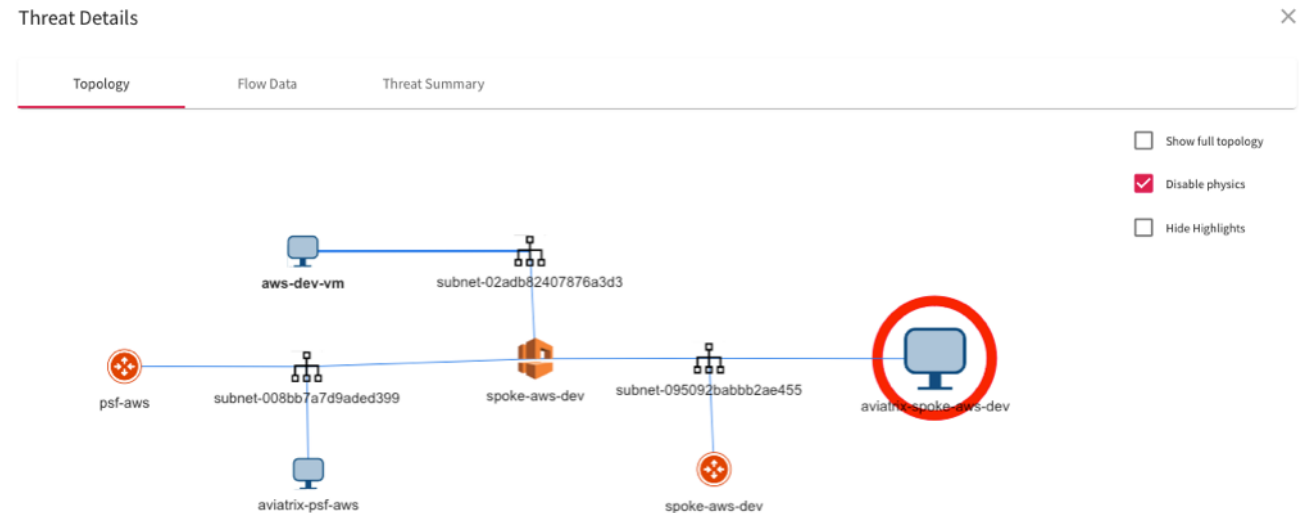
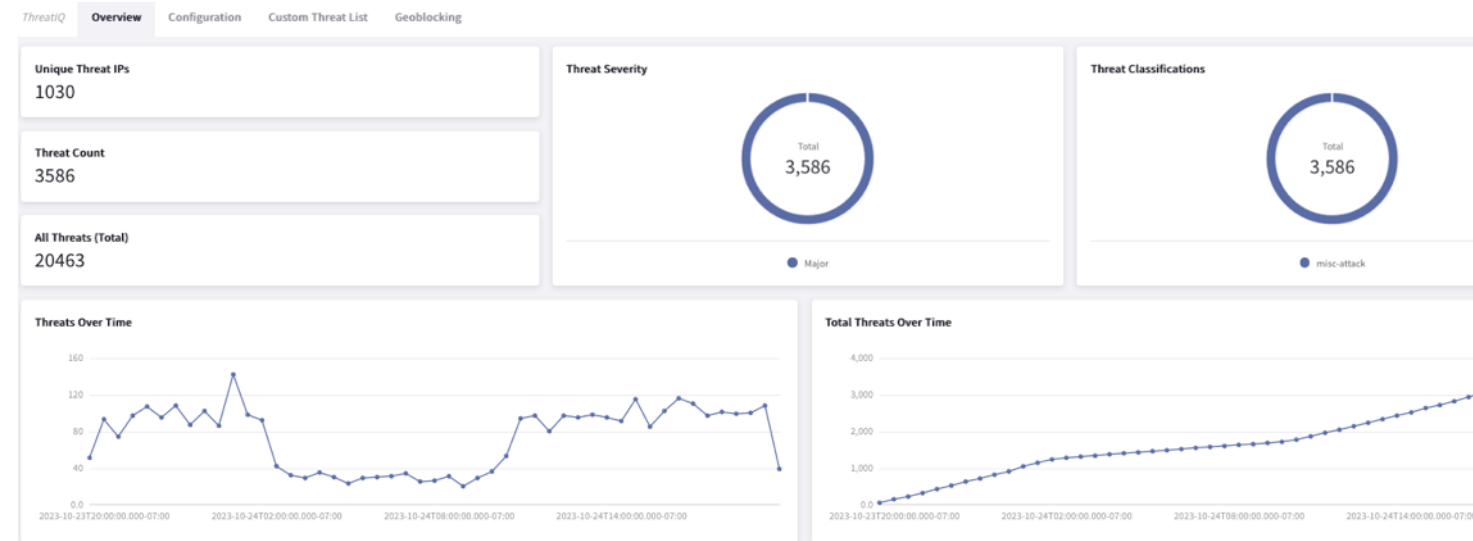


• Distributed Inspection & Notification

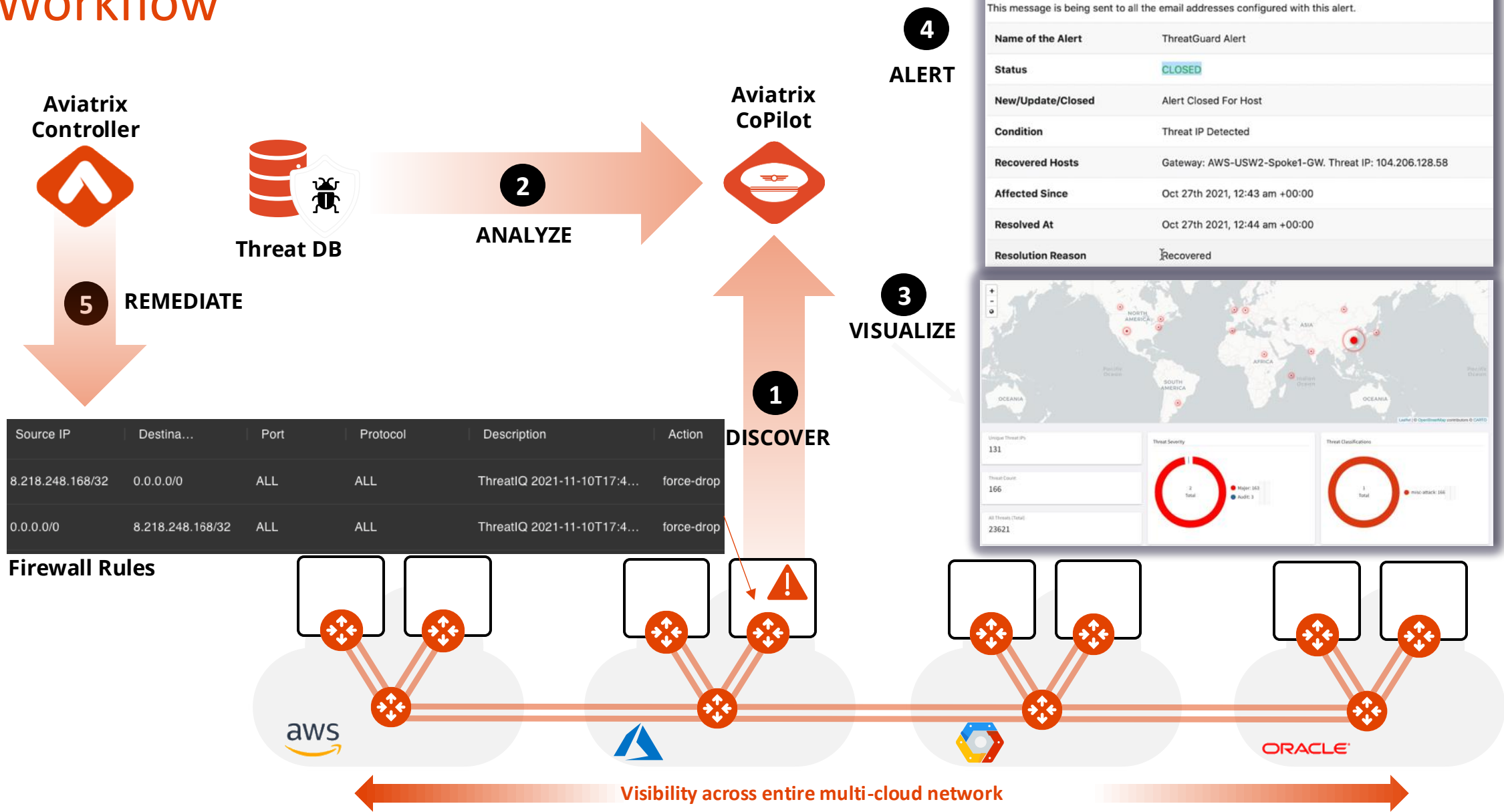
- Aviatrix gateways across Multicloud environment send real-time NetFlow data to CoPilot
- CoPilot analyzes the data on all public destinations against well-known Threat DB
- CoPilot alerts on any potential threats in the environment
- CoPilot provides extreme visibility of the impacted communication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





Block Threats Based on Geographic Location

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

☐ Show Only Blocked Countries



Countries	Status	IPs Observed (Last 7 Days)	
Argentina	<input type="checkbox"/> Allowed	12	
American Samoa	<input type="checkbox"/> Allowed		
Austria	<input type="checkbox"/> Allowed	33	
Australia	<input type="checkbox"/> Allowed	87	
Aruba	<input checked="" type="checkbox"/> Blocked		
Åland Islands	<input type="checkbox"/> Allowed		
Azerbaijan	<input type="checkbox"/> Allowed	26	
Bosnia and Herzegovina	<input type="checkbox"/> Allowed		
Barbados	<input type="checkbox"/> Allowed		
Bangladesh	<input type="checkbox"/> Allowed	79	
Belgium	<input type="checkbox"/> Allowed	55	
Burkina Faso	<input type="checkbox"/> Allowed		
Bulgaria	<input type="checkbox"/> Allowed	3'106	



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



Total Anomalies

1634

VPC/VNets with Anomalies

5

Metrics causing Anomalies

8

Anomalies by Severity



- Low
- Medium
- High

Anomalies by VPC/VNet



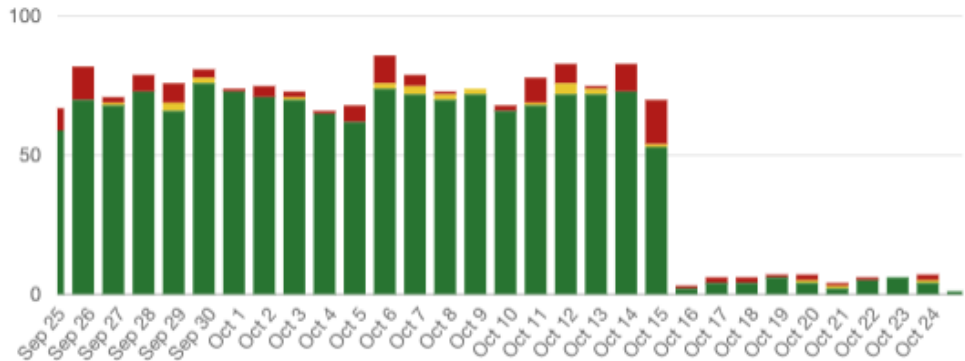
- accounting-aws-spok...
- engineering-aws-spok...
- marketing-azure-spok...
- operations-oci-spoke...
- enterprise-data-gcp-s...

Anomalies by Top Metric



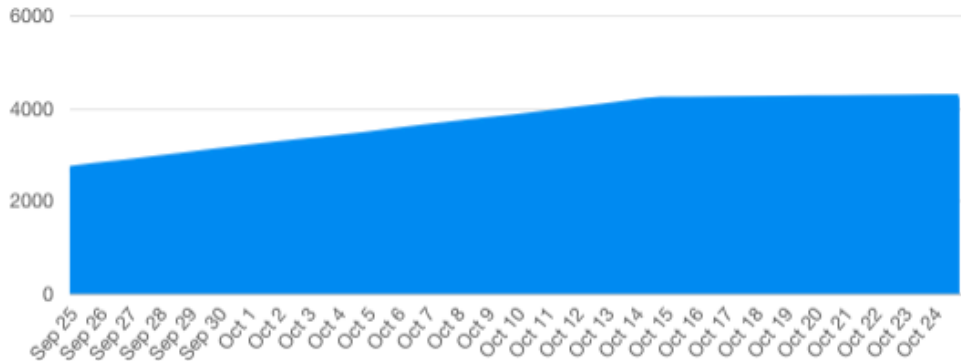
- Number of Egress Ports
- Number of Ingress Ports
- Egress Bytes
- Total Packets
- Total Bytes
- Number of Ingress IPs
- Ingress Bytes

Anomalies Over Time



1 Month

Total Anomalies (Cumulative)



1 Month

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	<input checked="" type="checkbox"/>
Oct 8, 2023 3:00:11 PM	engineering-aws-spoke-dev	AWS	3	Low	<input checked="" type="checkbox"/>

Manage Monitored VPC/VNets

☐ Available
0/6 selected

Filter

VPC/VNet Name	Cloud	Region
<input type="checkbox"/> lv-metro-megaport-edge-site	aviatrix	avx-edge-default
<input type="checkbox"/> operations-aws-spoke-landing-z	aws	us-east-1
<input type="checkbox"/> No Name	aws	us-east-2
<input type="checkbox"/> sv-metro-equinix-demo-edge-site	aviatrix	avx-edge-default
<input type="checkbox"/> example-azure-spoke-vnet	arm	East US
<input type="checkbox"/> example-aws-spoke-vpc	aws	us-east-1



☐ Monitored
0/16 selected

Filter

VPC/VNet Name	Cloud	Region
<input type="checkbox"/> accounting-aws-spoke-dev	aws	us-east-1
<input type="checkbox"/> accounting-aws-spoke-prod	aws	us-east-1
<input type="checkbox"/> accounting-aws-spoke-qa	aws	us-east-1
<input type="checkbox"/> engineering-aws-spoke-dev	aws	us-east-2
<input type="checkbox"/> engineering-aws-spoke-prod	aws	us-east-2
<input type="checkbox"/> engineering-aws-spoke-qa	aws	us-east-2
<input type="checkbox"/> enterprise-data-gcp-spoke-dev	gcp	us-west1
<input type="checkbox"/> enterprise-data-gcp-spoke-prod	gcp	us-west1
<input type="checkbox"/> 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

Anomaly Detection

Configuration	Monitored VPC/VNets
<p>1. Network Configuration</p> <ul style="list-style-type: none"> 1.1. VPC/VNet ID 1.2. Subnet ID 1.3. IP Address Range 1.4. Route Table 1.5. Internet Gateway 1.6. NAT Gateway 1.7. Elastic IP Address 1.8. Security Group 1.9. Network ACL 1.10. VPC/VNet Peering 	<p>2. Resource Configuration</p> <ul style="list-style-type: none"> 2.1. EC2 Instance 2.2. S3 Bucket 2.3. IAM Role 2.4. Lambda Function 2.5. RDS Instance 2.6. ElastiCache Instance 2.7. IAM User 2.8. IAM Group 2.9. IAM Policy 2.10. IAM Role 2.11. IAM User 2.12. IAM Group 2.13. IAM Policy 2.14. IAM Role 2.15. IAM User 2.16. IAM Group 2.17. IAM Policy 2.18. IAM Role 2.19. IAM User 2.20. IAM Group 2.21. IAM Policy 2.22. IAM Role 2.23. IAM User 2.24. IAM Group 2.25. IAM Policy 2.26. IAM Role 2.27. IAM User 2.28. IAM Group 2.29. IAM Policy 2.30. IAM Role 2.31. IAM User 2.32. IAM Group 2.33. IAM Policy 2.34. IAM Role 2.35. IAM User 2.36. IAM Group 2.37. IAM Policy 2.38. IAM Role 2.39. IAM User 2.40. IAM Group 2.41. IAM Policy 2.42. IAM Role 2.43. IAM User 2.44. IAM Group 2.45. IAM Policy 2.46. IAM Role 2.47. IAM User 2.48. IAM Group 2.49. IAM Policy 2.50. IAM Role 2.51. IAM User 2.52. IAM Group 2.53. IAM Policy 2.54. IAM Role 2.55. IAM User 2.56. IAM Group 2.57. IAM Policy 2.58. IAM Role 2.59. IAM User 2.60. IAM Group 2.61. IAM Policy 2.62. IAM Role 2.63. IAM User 2.64. IAM Group 2.65. IAM Policy 2.66. IAM Role 2.67. IAM User 2.68. IAM Group 2.69. IAM Policy 2.70. IAM Role 2.71. IAM User 2.72. IAM Group 2.73. IAM Policy 2.74. IAM Role 2.75. IAM User 2.76. IAM Group 2.77. IAM Policy 2.78. IAM Role 2.79. IAM User 2.80. IAM Group 2.81. IAM Policy 2.82. IAM Role 2.83. IAM User 2.84. IAM Group 2.85. IAM Policy 2.86. IAM Role 2.87. IAM User 2.88. IAM Group 2.89. IAM Policy 2.90. IAM Role 2.91. IAM User 2.92. IAM Group 2.93. IAM Policy 2.94. IAM Role 2.95. IAM User 2.96. IAM Group 2.97. IAM Policy 2.98. IAM Role 2.99. IAM User 2.100. IAM Group

Monitored VPs




16  

Time Period

Last 7 Days

Total Anomalies

Anomalies by Seve

<div> <div>    </div> <div> <input type="text" value="Search"/> </div> </div>				
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-dev	Gcloud	us-west1	Complete	Active
enterprise-data-gcp-spoke-prod	Gcloud	us-west1	Complete	Active
enterprise-data-gcp-spoke-qa	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



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



COMMUNITY
<https://community.aviatrix.com>