The Cloud Pragmatist | Secure Cloud Networking

Protect your multi-cloud infrastructure with these must-have components:

End-to-End Encryption

High-performance, end-to-end encryption between VPCs/VNets and between clouds, meeting or exceeding corporate and regulatory requirements.

Multi-Cloud Network Segmentation

Secure network segmentation with consistent firewalling across clouds and extending beyond cloud boundaries.

Threat Intelligence Feeds

TI feeds across network for real-time data streams of potential or immediate risks that could impact any node in the multi-cloud architecture.

Status of internet access confirmed across all CSPs.

Secure Cloud Ingress/Egress Controls

Gateways providing ingress/egress L4 and Fully Qualified Domain Name (FQDN) filtering.

Centrally managed filter groups ensuring consistent multi-cloud security for any cloud application communicating with internet-based resources and services.

Multi-Cloud Network Service Insertion

Secure point-of-access for network and security services such as next-generation firewalls, IDS/IPS and SD-WAN cloud edge connections.

Operational Visibility

Multi-cloud network topology map includes both native network resources and secure transit and cloud ingress/egress control gateways.

Visibility to network traffic flow including source, destination, port and protocol filtering.

Procedures for network and application team collaboration, using detailed analysis of traffic and systems that connect application endpoints, including gateway performance, network latency, route table analysis and security domains.

Automated Remediation Capabilities

Remediation capabilities automated to save time and resources.

Automated remediation incorporates security across architecture, protecting every network node.

aviatrix