AVIATRIX®

Cloud Native Security Fabric

Characteristics

Aviatrix Cloud Native Security Fabric: The Missing Control Layer

In today's multicloud landscape, security teams face a critical challenge: traditional security tools weren't built for cloud-native architectures. Aviatrix Cloud Native Security Fabric (CNSF) bridges this gap by providing a holistic, unified security solution designed specifically for complex and distributed networks spanning multiple clouds and on-premises environments.

Cloud Expertise Development

The Challenge

Identifying what's required for secure cloud networking

The Approach

Cloud experts collaborating intensively for a week

The Outcome

Comprehensive cloud reference architecture

Seven years ago, Aviatrix assembled a team of cloud networking specialists to tackle a fundamental question: **"What would you need to do secure cloud networking in the cloud as far as a reference architecture is concerned?"** Through intensive collaboration, these experts developed a groundbreaking reference architecture that would serve as the foundation for the CNSF.

Seven Ways CNSF Complements Your Security Stack

Aviatrix CNSF doesn't replace your existing security tools—it fills critical gaps and enhances their effectiveness. Here's how it addresses vulnerabilities that traditional security solutions miss in cloud environments.

1

Runtime Security That Works in Real-Time

Unlike CNAPPs and CSPMs that analyze security posture after events occur, Aviatrix operates at ***runtime***. Through network-wide visibility and anomaly detection, it identifies suspicious activity as it happens and enforces security policies to shut down attacks in flight—before damage occurs.

2

Network Segmentation to Stop Lateral Movement

CNSF prevents attackers from moving laterally through your infrastructure by ***segmenting*** networks and workloads. It enforces consistent security policies within and across VPCs, VNets, and clouds—unlike SASE and SSEs that leave gaps for attackers to exploit as they collect and exfiltrate data.

3

Secure Local Egress Without Backhauling

Even when attackers disable EDRs or bypass other security solutions, they must eventually exfiltrate stolen data. Aviatrix stops data exfiltration using advanced ***egress security*** and network-wide visibility—detecting and blocking exfiltration attempts without requiring expensive traffic backhauling to centralized inspection points.

4

Identity-Aware Policies Based on Workload Metadata

CNSF bases security policies on ***workload identity*** using metadata like tags rather than IP addresses or CIDR blocks. This approach eliminates security holes created by misconfigured IP-based policies or overlapping IP address spaces across multiple cloud environments.

5

High-Performance Encryption Breaking Speed Barriers

Aviatrix *High-Performance Encryption (HPE)* is a proprietary solution that delivers high-speed encryption beyond the legacy 1.25 Gbps limit of traditional approaches. Unlike MACsec, it avoids MITM exposure, providing stronger security and higher throughput.

6

Enterprise-Grade Visibility and Diagnostic Tools

Moving to the cloud meant losing traditional network diagnostic capabilities. *Aviatrix Policy Enforcement Points* restore familiar tools like ***ping, traceroute, tcpdump, and netflow***, while introducing cloud-native innovations like *FlightPath* for comprehensive network troubleshooting and analysis.

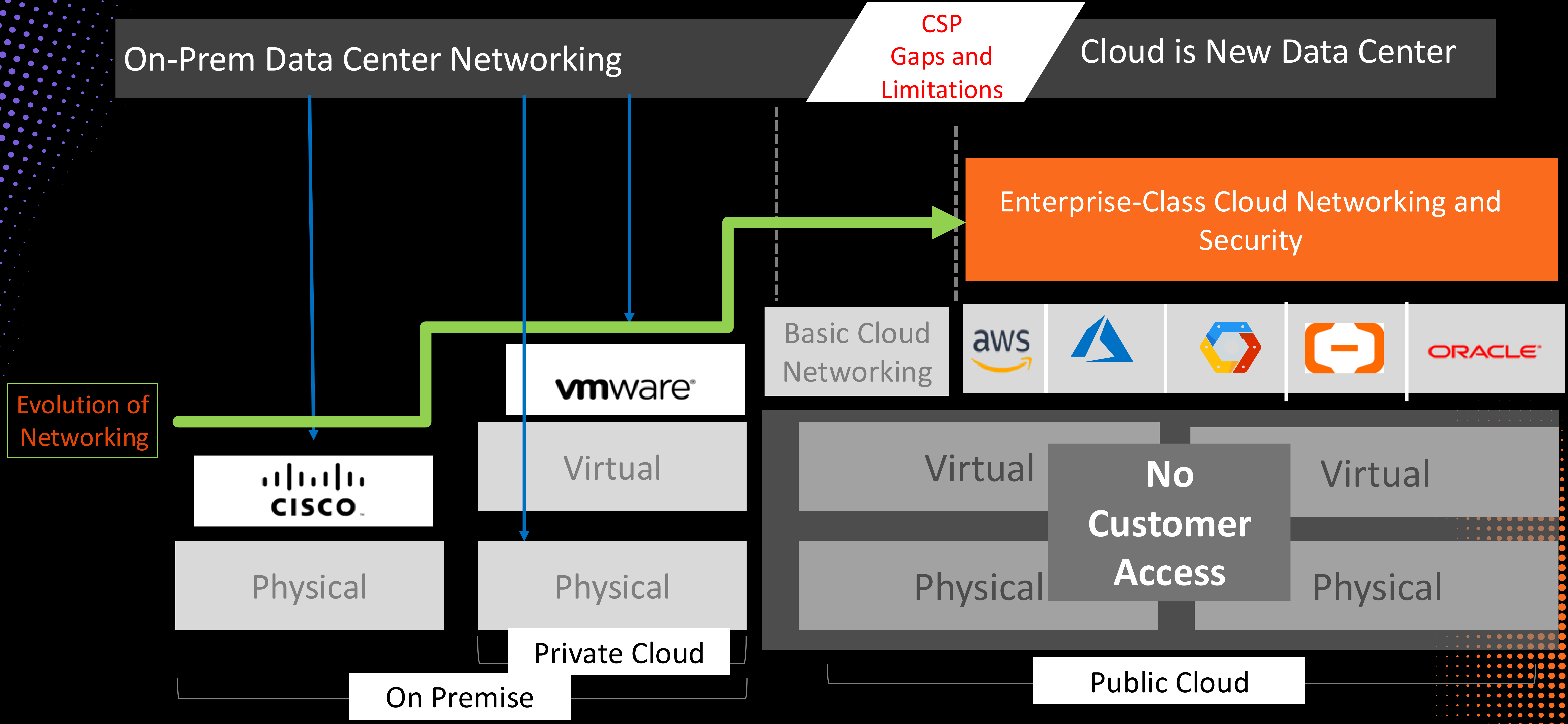
7

Multicloud Orchestration from a Single Console

Configuring security and network elements across multiple clouds typically requires coordination between multiple teams over days or weeks. Aviatrix provides *a single pane of glass* for orchestrating multicloud infrastructure in minutes—with Terraform automation support to streamline deployment and eliminate connectivity bottlenecks.

AVIATRIX

CSP Networking Has Gaps | You need a Secure Fabric



On-Prem Data Center Networking

CSP Gaps and Limitations

Cloud is New Data Center

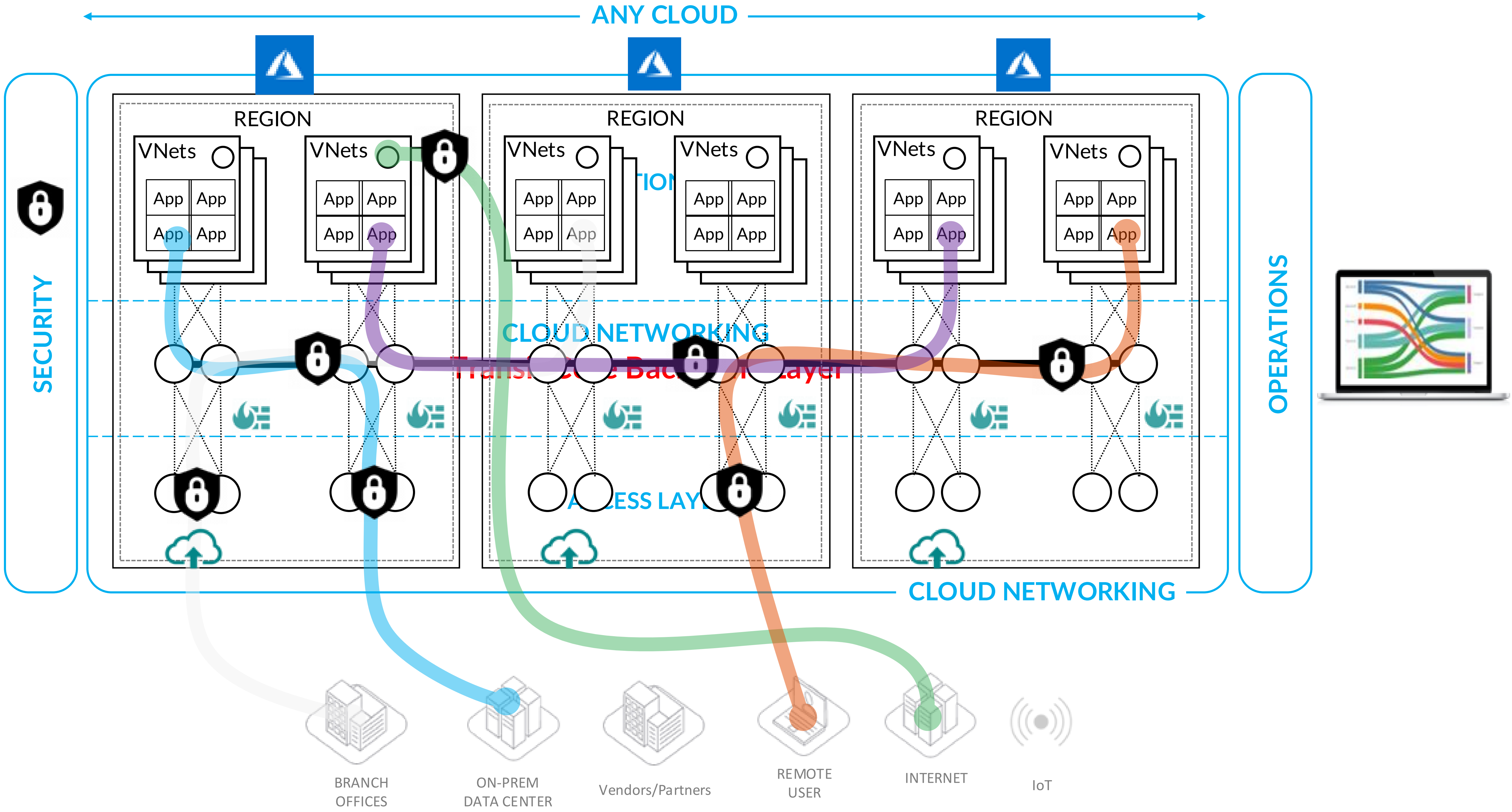
Enterprise-Class Cloud Networking and Security

Evolution of Networking

AVIATRIX

CNSF (Single Cloud)

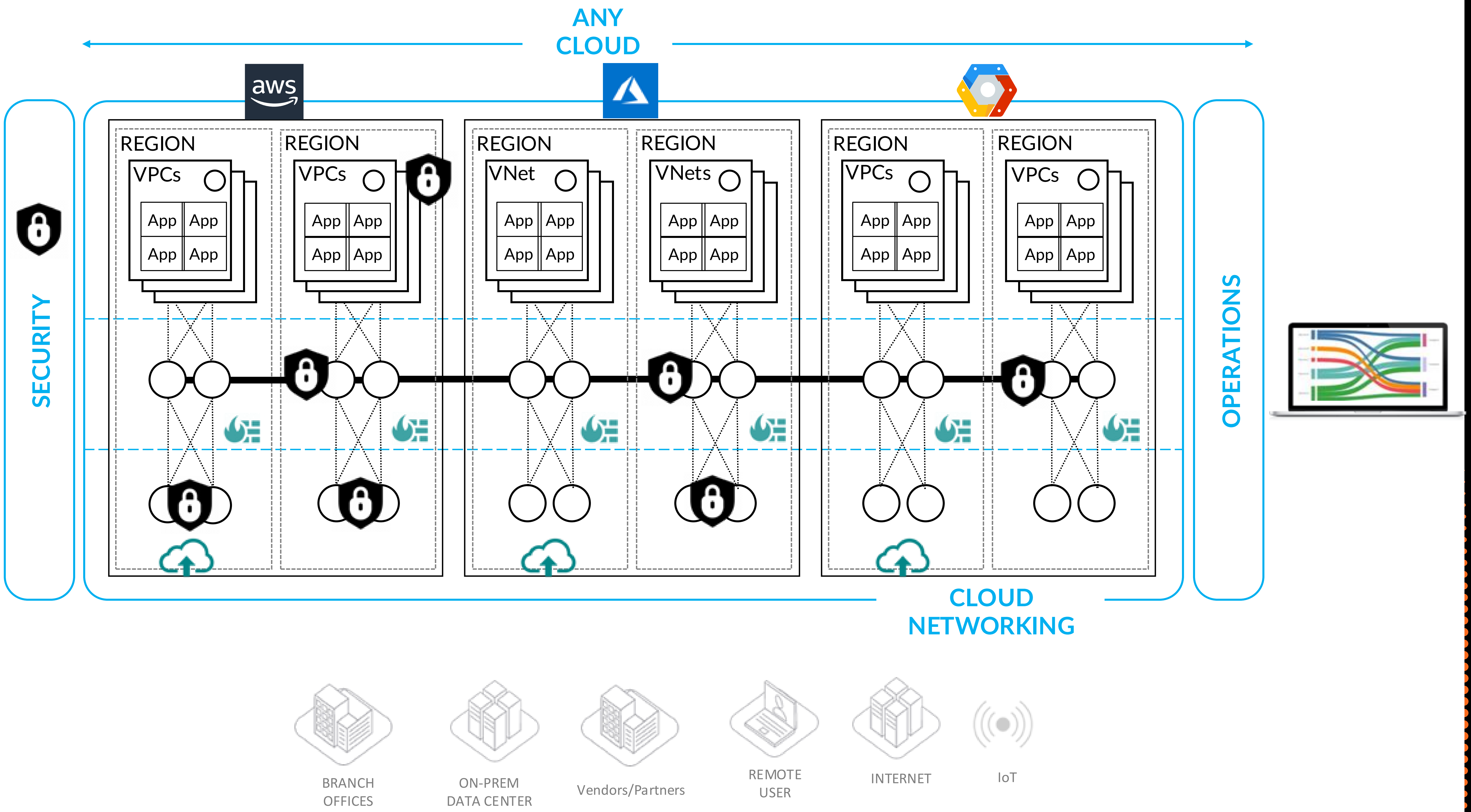
- Single Cloud, Multi-Region, Multi-Account
- Repeatable Network Design and Infrastructure as Code Automation
- Service Insertion and Chaining
- De facto Cloud Firewall
- Common Operational Visibility and Control



AVIATRIX

CNSF (Multicloud)

- Multicloud, Multi-Region, Multi-Account
- Repeatable Network Design and Infrastructure as Code Automation
- Service Insertion and Chaining
- De facto Cloud Firewall
- Common Operational Visibility and Control



Next: CNSF - Deployment