



# CREATING AN ENTERPRISE-READY MULTI-CLOUD STRATEGY:

A Guide to Simplifying  
Enterprise Cloud Networking



---

# CONTENT

## 3

### INTRODUCTION

- MULTI-CLOUD SIMPLICITY
- CLOUD EVOLUTION DRIVES MULTI-CLOUD
- THE MULTI-CLOUD MARKET BY THE NUMBERS

## 8

### ENTERPRISE CHALLENGES ACROSS THE CLOUD

- ENTERPRISE CHALLENGES WITHIN THE CLOUD

## 11

### WHY ARE ENTERPRISES IMPLEMENTING A MULTI-CLOUD STRATEGY?

- WHAT SHOULD AN ENTERPRISE MULTI-CLOUD STRATEGY LOOK LIKE?

## 16

### EPSILON CLOUD NETWORKING

- SOLUTION COMPONENTS
- DIFFERENTIATORS
- WHY IT MATTERS
- EPSILON'S CLOUD NETWORKING BENEFITS

## 24

### TECHNICAL USE CASES

- NEW GCP CUSTOMER
- AWS/AZURE CUSTOMER EXTENDING TO GCP

## 29

### MOVING FORWARD WITH MULTI-CLOUD



Public cloud adoption is rapidly accelerating. According to Gartner, worldwide end-user spending on public cloud services is forecast to grow 18.4% in 2021 to total \$304.9 billion, up from \$257.5 billion in 2020. On top of this, the proportion of enterprise IT spending that is shifting to cloud is on the rise due to COVID-19, with cloud projected to make up 14.2% of the total global enterprise IT spending market in 2024, up from 9.1% in 2020.

A key reason that enterprises do not achieve expected return on investment (ROI) in cloud is due to operational and network complexity. Some enterprises still follow the 'lift and shift' approach, building their cloud deployments the same way as they were doing for years in the on prem world. This is preventing enterprises from really benefitting from the scalable cloud model.

Resources in the clouds need to be created and torn down depending on the actual needs of users. This requires automation across all layers, from networking right up to the application layer. Customers need to accept that VPCs/VNETs/VCNs can be very dynamic entities, and they need to be prepared to handle provisioning of their networking resources in a fully automated way to keep up with the needs of their applications.





## MULTI-CLOUD SIMPLICITY

Enterprises are increasingly using any and every cloud provider to achieve the full flexibility and benefits of the cloud. With more enterprises embracing this multi-cloud model, they need to understand how to connect their clouds and unleash their full potential.

Utilising a Multi-Cloud model can be the key to solving enterprise challenges in the cloud, as well as enhancing operations, application performance and helping to keep up in a changing market. With more interworking between clouds in a single environment, enterprises need simpler management of the multi-cloud environment. They need to look at the simplest model for connecting multiple clouds, distributing resources, mitigating downtime and minimising data loss risk.





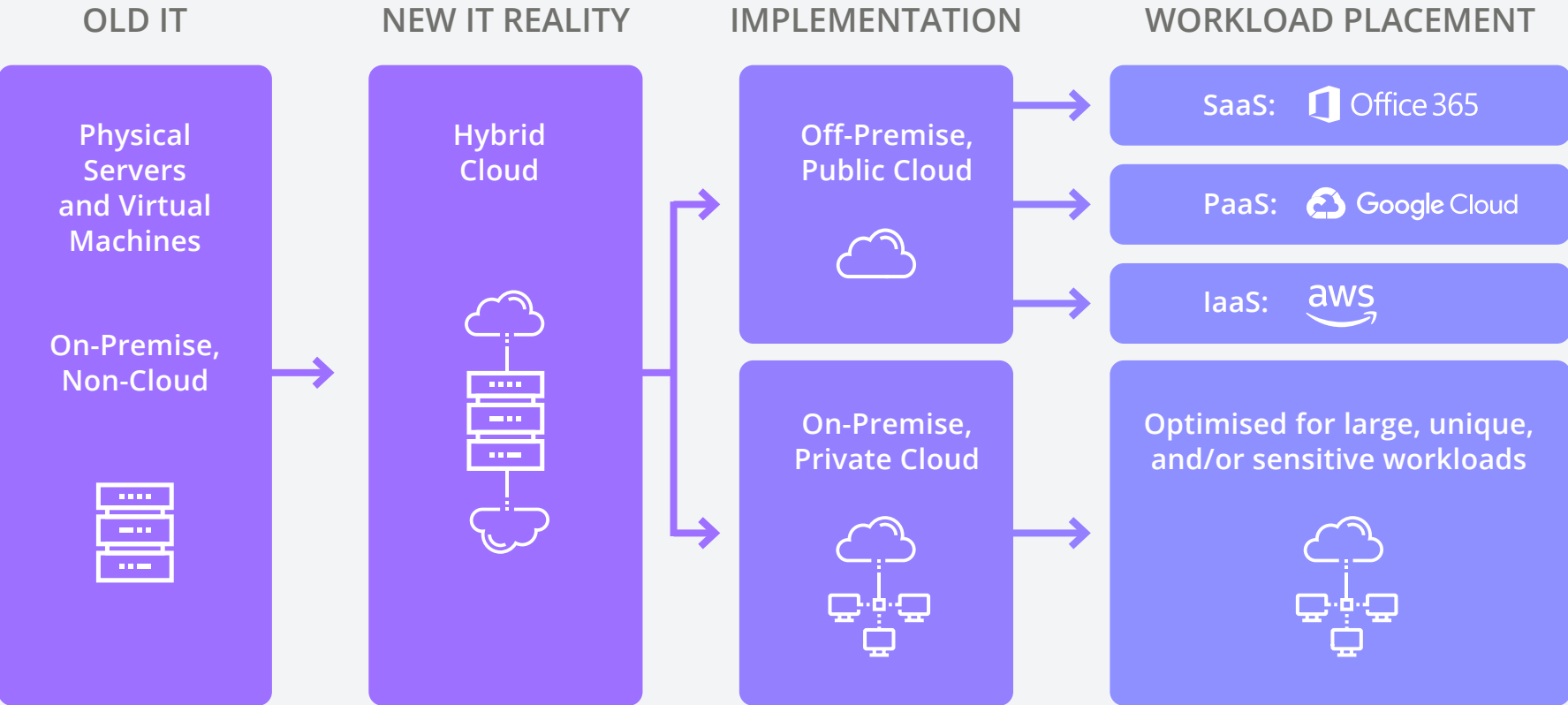
## CLOUD EVOLUTION DRIVES MULTI-CLOUD

A multi-cloud strategy is the use of two or more cloud computing services. While a multi-cloud deployment can refer to any implementation of multiple software as a service (SaaS) or platform as a service (PaaS) cloud offerings, today, it generally refers to a mix of multiple public or private cloud environments, such as Amazon Web Services, Microsoft Azure, Google Cloud Platform and on and off premise private cloud.





Unlike old IT models, many enterprises are implementing a mix of public clouds and also private cloud for the appropriate workloads or applications. With more interworking between clouds in a single environment, enterprises will need simpler management of the entire IT workloads.





## THE MULTI-CLOUD MARKET BY THE NUMBERS



“ **By 2022, over 90%** of enterprises worldwide will be relying on a mix of on-premises/dedicated private clouds, multiple public clouds, and legacy platforms to meet their infrastructure needs. ”

**IDC**



“ The multi-cloud management market is expected to grow from approximately \$1.2 billion in 2017 to **\$4.5 billion by 2022**, at a Compound Annual Growth Rate (CAGR) of **30.9%** from 2017 to 2022. ”

**MARKETSANDMARKETS**

# ENTERPRISE CHALLENGES ACROSS THE CLOUD







Enterprises are facing a whole range of challenges when it comes to cloud. Those running on a single cloud are limited to its native constructs, which causes limitations that are not even aware of. When scaling their businesses, they will face challenges in connecting their architectures without the right model.



**ARCHITECTURE GAP** – If they choose to extend to other clouds, they cannot use the same set of architecture to replicate the same design in the other clouds. This means they have to re-work their entire architecture, due to a lack of common control and data plane.



**MULTI-CLOUD NETWORKING** – Most of the main cloud service providers (CSP) are not interested in making it easy to expand to other cloud providers. Enterprise can take a multi-cloud approach to avoid lock-in and also better cost management.



**COMPLEXITY & SKILLS GAP** – Each cloud has unique networking capabilities and limitations, which require skills and knowledge specific to the CSP. Not all enterprises possess the ability to deploy and manage these environments.



**LACK OF CENTRALISED CONTROLLER** – Most hyperscalers do not provide any form of cloud network platform to program both native cloud network constructs and advanced services. Enterprise do not have control over the network and security automation services across their multi-cloud environment.



**BASIC NETWORKING FEATURES** – When an enterprise chooses a hyperscaler for its cloud services, it will have to manage its own networking and security. Such services often lack visibility into real-time network data and analytics, as well as offering little control in terms of availability and encryption.



# ENTERPRISE CHALLENGES WITHIN THE CLOUD

Within the cloud, another set of challenges arise for enterprises.

**CLOUD INTEGRATION** – Enterprises face networking issues associated with having their on-premises apps and tools, legacy systems and clouds to work together. Combining native cloud constructs with standard WAN networking requires resources, expertise and time.

**LACK OF VISIBILITY** – Cloud-native construct do not give networking or security team visibility into packet flows. When cloud networks sprawl multiple regions, the likelihood of an adverse network event increase.



**LIMITED SECURITY** – End-to-end encryption for data in motion, secure network segmentation, policy-based ingress and egress control and both corporate and regulatory compliance and governance are all significant challenges for enterprises.

**MANUAL PROCESS** – It is difficult, error prone and resource intensive to manually configure and maintain an enterprise cloud network environment of any significant size.

WHY ARE  
ENTERPRISES  
IMPLEMENTING  
A MULTI-CLOUD  
STRATEGY?





Enterprises must be able to scale up or down according to varying market demands.

While public cloud platforms provided by hyperscalers provide this agility and scalability, enterprise have limited choices in terms of regions and availability zones.

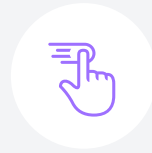
A multi-cloud approach can include a mixture of on-premise/private clouds, public clouds, and even legacy platforms to ensure performance, security and 24/7 availability. Here are the reasons why:





### ORCHESTRATING NEW DATA AND APPLICATIONS

Many businesses are now using multiple public clouds for their data and applications. They need the capability to efficiently coordinate disparate workloads, manage workflows and integrate processes. A multi-cloud solution enables the orchestration of data, applications and infrastructure across several cloud environments. It simplifies cloud deployment by connecting applications and workflow processes to quickly deliver business services.



### AVOID VENDOR LOCK-IN

Most organisations adopt a multi-cloud strategy to fully harness the power of the cloud by taking advantage of best-of-breed services. For instance, an enterprise might be using Amazon Web Services for its compute services and Oracle Cloud for its database solutions. Businesses should have the freedom to switch from one cloud provider as their business and IT needs evolve.



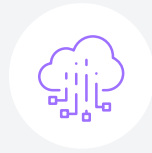
### RISK MITIGATION

With a multi-cloud strategy, businesses can mitigate risks associated with infrastructure meltdown or an attack. They can quickly move their data and applications to another cloud provider or even back-up to a private cloud. Security features can also be implemented to ensure a robust risk management system in the multi-cloud environment.



### **DATA SOVEREIGNTY, LAW AND REGULATIONS**

For organisations in some countries, there are laws, regulations and corporate policies that require enterprise data to physically reside in certain locations. Multi-cloud allows organisations to meet those requirements as they are able to choose multiple cloud providers' data centre regions or availability zones.



### **FOCUS ON INNOVATION**

Each cloud provider has its strength and weaknesses. A multi-cloud approach allows you to choose the best cloud provider and services that best fit your business needs. It enables greater flexibility for businesses to innovate rapidly by taking advantage of unique sets of services offered by multiple cloud providers.



### **NETWORK AVAILABILITY AND PERFORMANCE**

A multi-cloud approach allows organisations to extend their networks to multiple cloud providers. They can interconnect distributed data centres that are in close proximity to their customers to achieve optimal performance and minimal latency. A highly optimised interconnection can be achieved through private connectivity between multiple cloud providers.



# WHAT SHOULD AN ENTERPRISE MULTI-CLOUD STRATEGY LOOK LIKE?

A multi-cloud strategy can offer enterprise-class cloud networking and security, as well as full operational visibility and control. With the right partner, enterprises can benefit from rapid deployment, expert support and continual transformation to take their cloud strategy to the next level. It should provide the following features to enterprises:



# EPSILON CLOUD NETWORKING







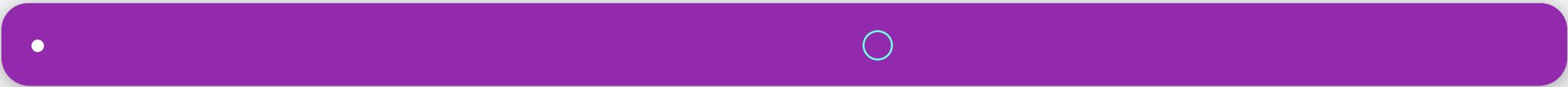
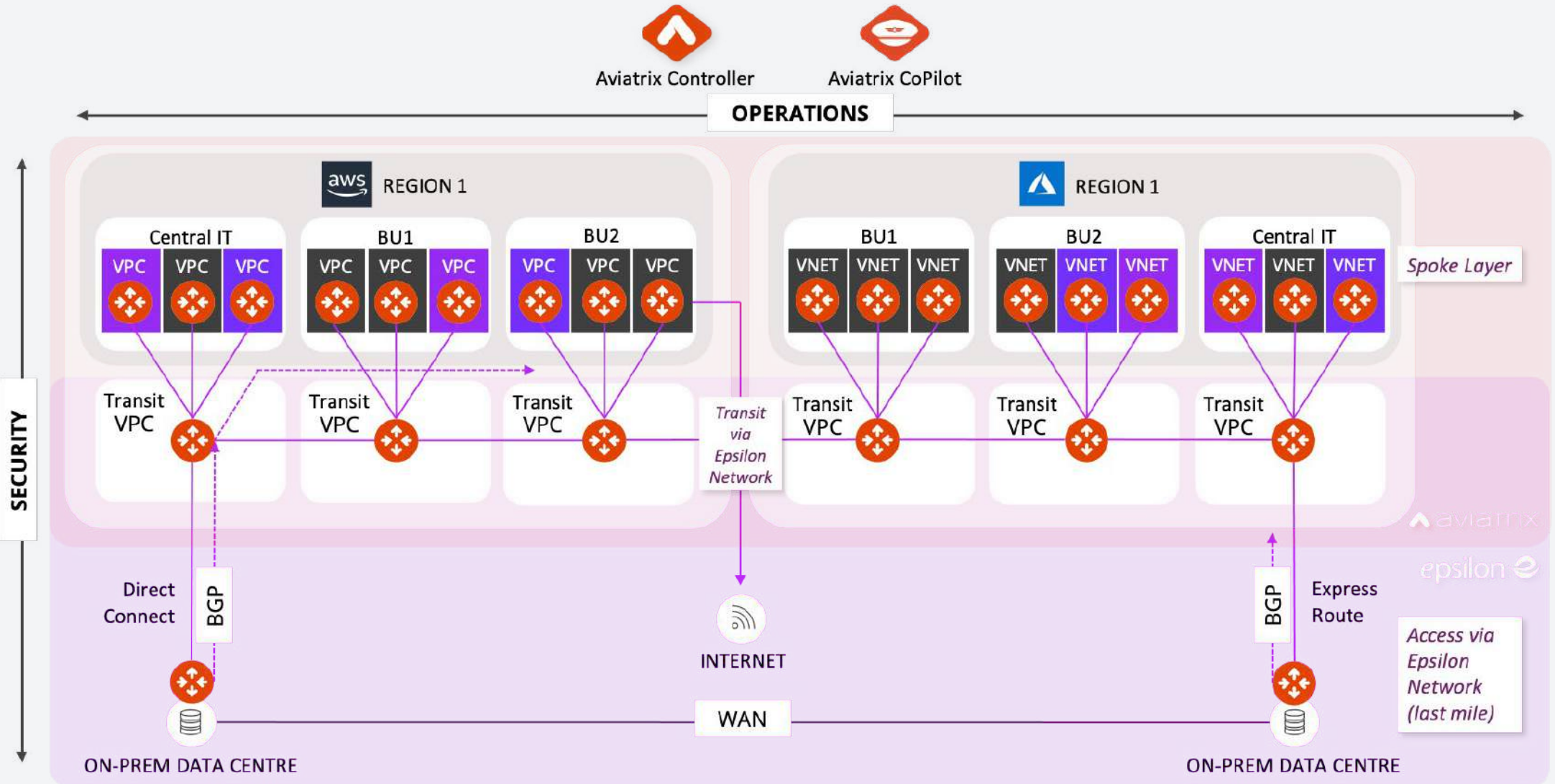
## EPSILON CLOUD NETWORKING

Epsilon has purpose-built a cloud networking solution that delivers a multi-cloud network platform with the simplicity, automation, operational visibility and control that enterprises need.

The solution provides a private network as underlay and the Aviatrix cloud network platform to create an enterprise-class network inside and between public clouds, up to the VPC/VNET level. It allows customers to consume security services, such as FQDN filtering and service insertion of next-gen firewalls, to meet their security and compliance requirements.

This provides a solid foundation for the future, moving enterprises from basic cloud connectivity to advanced enterprise-ready end-to-end multi-cloud network architecture.

# MULTI-CLOUD NETWORKING WITH OPERATIONAL VISIBILITY AND CONTROL



## MODULAR & FLEXIBLE DESIGN CHOICES

### EPSILON CLOUD NETWORKING FOUNDATION

- **Private network:** Connection to Clouds via Epsilon private network
- Single Cloud
- Multiple Clouds
- **Access:** Data centre, branch office, vendors/partners, remote users
- Any to any mesh networking
- All the way to VPC/VNET



Epsilon Private Network



Aviatrix Controller



Aviatrix CoPilot

**HIGH AVAILABILITY:** Dual gateways in active/active or active/backup

**ENCRYPTION:** Line-rate high-speed encryption, no 1.2Gbps IPsec limit

**ADVANCED NETWORKING:** Extends native public cloud capabilities and overcomes limitations

**REPEATABLE ARCHITECTURE:** Define a pod like design and apply it in same or different clouds

**OPERATIONAL EFFICIENCY:** Hitless-upgrades, zero downtime, FlightPath

### MODULAR ADD-ONS

Multi-cloud segmentation

UserVPN (remote users)

FQDN Filtering

Firewall Networks

Secure Ingress/Egress

SD-WAN integration



# SOLUTION COMPONENTS

**Epsilon Cloud Connect & Layer 3 Mesh Network** – Private network with Layer 3 (L3) access to cloud providers via cloud on-ramps and data centre/branch office connectivity. Epsilon private network to orchestrate routing between clouds, data centres and branch locations.

**Aviatrix Gateways** are used to deliver advanced networking and security features to augment and overcome native cloud limitations and lack of visibility.

**Aviatrix Co-Pilot** provides a global operational view of your multi-cloud network available from AWS, Azure or any other cloud providers. This is often used by enterprise IT teams who need day two operational visibility for cloud networking. They can use CoPilot to view and analyse global heat maps and time series trend charts to easily pinpoint and troubleshoot traffic anomalies.

**Aviatrix Controller** directly controls both native cloud constructs and Aviatrix Service Gateways via APIs to abstract complexities unique to each cloud and form a common multi-cloud network.



# DIFFERENTIATORS



## **Simplified Repeatable Cloud**

**Networking** – A simplified, repeatable cloud networking architecture across any cloud.

**Individual VPC/VNET** – Our solution goes beyond the cloud gateways all the way to VPC/VNET level.

## **High Performance Encryption**

Distributes processing across multiple cores and aggregates IPsec tunnel to achieve wirespeed encryption, up to 75 Gbps.

## **Visibility & Operations**

Advanced visibility and operations via controller FlowIQ – Intelligence Network Traffic Flow Analytics.

## **Epsilon Private Network**

Enterprise-class solution with embedded security using Epsilon private network as underlay and Aviatrix controller as overlay.

## **High Availability Networking**

High availability networking with full resiliency in both overlay and underlay network.

## **Multi-Cloud Segmentation**

Extends secure network segmentation beyond cloud boundaries, enabling multi-cloud security domains, with consistent, centrally managed, global network segmentation policy.



## WHY IT MATTERS



### **Solid Foundation for Your Future**

We move you from basic cloud connectivity to advanced enterprise-class end-to-end (up to VPC/VNET) multi-cloud network architecture, allowing you to manage your VPC/VNETs within a cloud and between clouds. Enterprise-class solution with embedded security using Epsilon's private network as underlay and Aviatrix's controller as overlay. High availability networking with full resiliency in both overlay and underlay network.

### **No More Blind Spots**

Multi-cloud visibility is simply not available from any other cloud provider. We offer you the tools to gain actionable intelligence of network health, traffic flows, anomalies and troubleshooting, within the cloud and between clouds, in minutes. Our team of cloud experts are at hand 24/7 to offer help and support.

### **Fully Managed Services**

A multi-cloud solution should not just connect your network to cloud gateways and leave open the inherent challenges of networking/security within the cloud. We provide you a fully managed (up to VPC/VNET level) consistent multi-cloud design that is repeatable across any public cloud. Aviatrix extends secure network segmentation beyond cloud boundaries, enabling multi-cloud security domains, with a consistent, centrally managed, global network segmentation policy.





# EPSILON'S CLOUD NETWORKING BENEFITS

**Fast Deployment** – Our Cloud Networking solution accelerates cloud network deployments to support the pace of business and app owners. You can move faster to meet demands at the click of a button.

**Full Control** – Deliver a multi-cloud network architecture with a common network data and operational control plane, to give you the control you need to succeed.

## **Security & Troubleshooting**

– Easily solve multi-cloud networking, security, visibility, and troubleshooting challenges that enterprise IT faces every day.

**Simple & Visible** – Through a single pane of glass, you can view your entire cloud network and simplify your cloud network operations. Gain full visibility to identify and resolve problems rapidly.

**Operational Visibility & Reduced MTTR** – 14x reduction time to plan, build and deploy tasks, and a 7x reduction time on Day-Two operational task.



# TECHNICAL USE CASES







## LEADING PROVIDER OF SECURITY AND INTELLIGENT DATA MINING SOFTWARE

### NEW GCP CUSTOMER

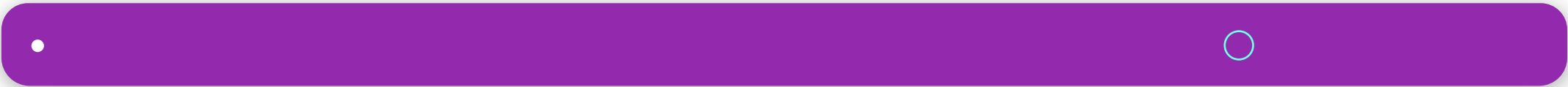
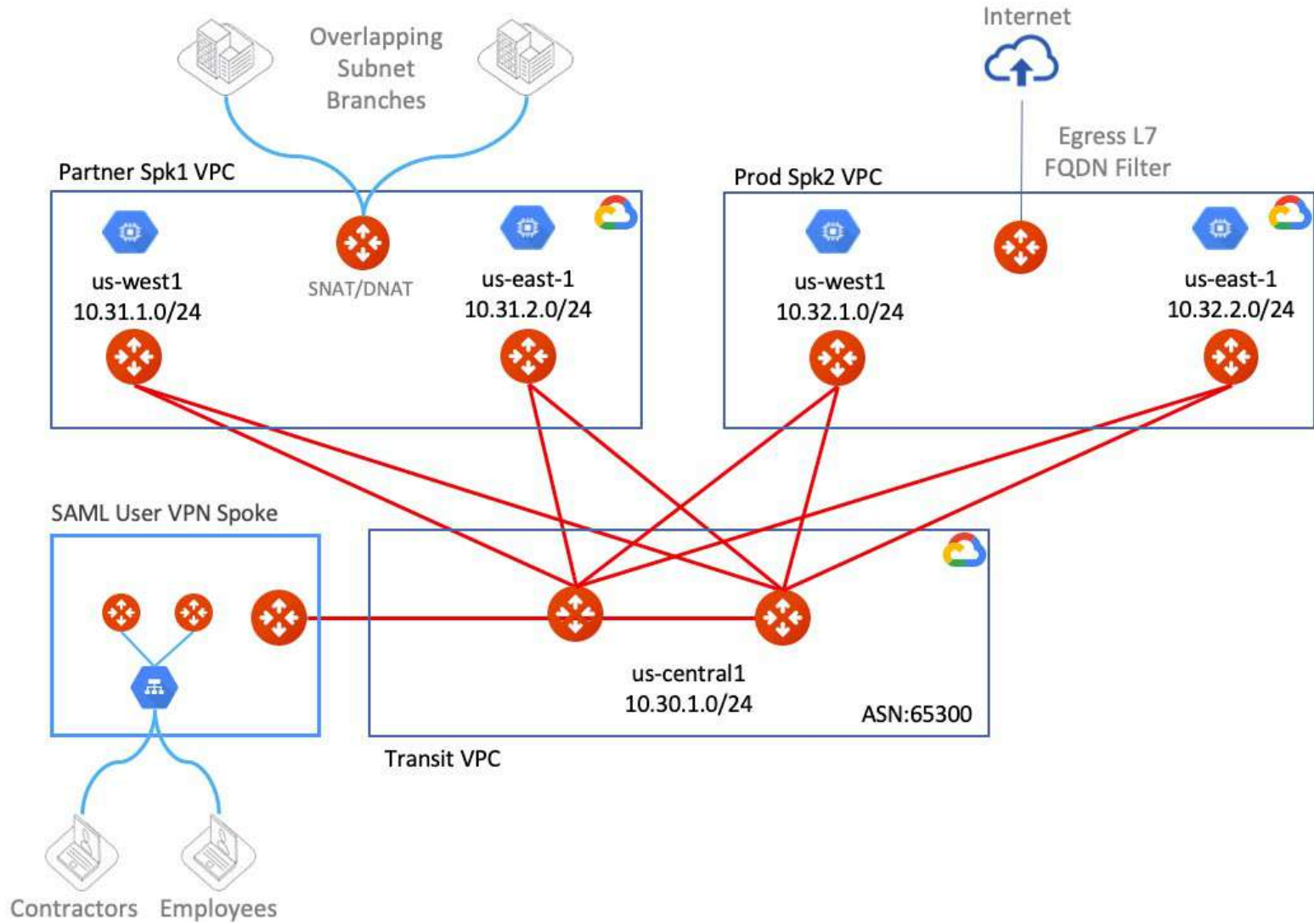


#### PAIN POINTS

- On-boarding environment was taking too long
- Maintaining compliance across multiple tenants
- Troubleshooting was lengthy and resource consuming process

#### SOLUTIONS

- Deployment automation, reduce customer on-boarding time
- Advance SNAT/DNAT to overcome overlapping IP challenge
- Secure L7 FQDN filtering
- Policy based SAML remote user access





## PROVIDER OF AI-BASED CYBER SECURITY SOFTWARE FOR INTERNET USERS & BUSINESSES. B2B SERVICES MODEL.

### AWS/AZURE CUSTOMER EXTENDING TO GCP

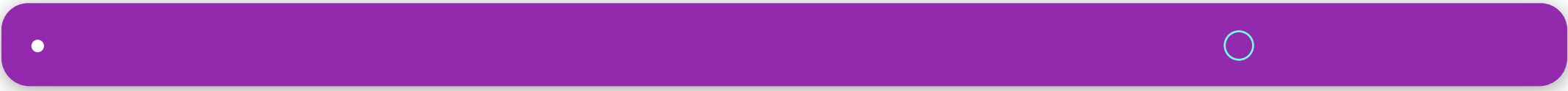
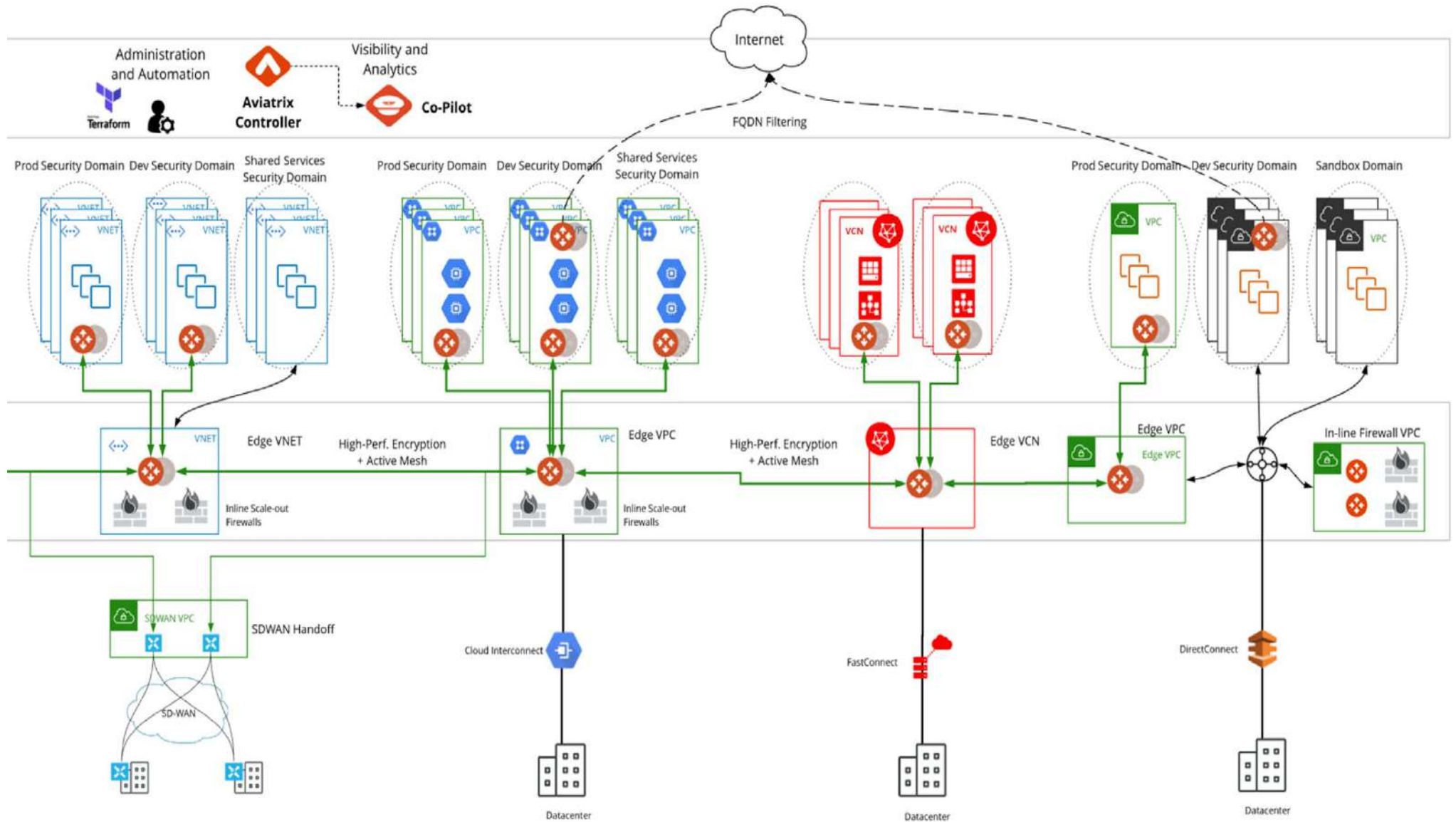


#### PAIN POINTS

- Common global standard for networking across multiple clouds
- Meet European Union compliance requirement
- Time to market services is critical

#### SOLUTIONS

- Aviatrix global & encrypted network across GCP, Azure & AWS
- Multi-cloud network segments for compliance
- SAML base User-VPN for developers to build app





## MOVING FORWARD WITH MULTI-CLOUD

Multi-cloud doesn't have to be complex. The right solution and expertise can provide a solid foundation for the future, moving enterprises from basic cloud connectivity to an advanced enterprise-class end-to-end multi-cloud network architecture. It should provide a fully managed and consistent multi-cloud design that is repeatable across any public cloud.

Multi-cloud is the key to unlocking the future of your business with advanced security, visibility and control. Simplify your multi-cloud journey with a comprehensive solution, so you are ready to keep up with competitors and move forward with confidence in a rapidly changing business environment.

**Speak with us about your cloud transformation needs**

Europe: +44 207 096 9600 | Asia: +65 6813 4020

[epsilonintel.com](http://epsilonintel.com) • [info@epsilonintel.com](mailto:info@epsilonintel.com)