aviatrix®

WHITEPAPER

9 Cloud Perimeter Security Challenges Solved with Aviatrix

Cloud environments are complex, with a lot of moving parts. This makes the critical function of securing the cloud perimeter challenging enough as it is. But there are a lot of levers that affect not just your security posture, but also costs, performance, agility, and more.

Think about your entire cloud estate and ask yourself the following questions:

- Is security applied inconsistently?
- Are your management capabilities fragmented?
- Is compliance a manual, time-consuming effort?
- Are your virtualized hardware appliances too costly?
- Are interruptions too frequent and last too long?
- Are data egress costs too high?
- Is overprovisioning driving up costs?
- Are your cloud visibility and monitoring fragmented?
- Is it hard to scale to accommodate evolving needs and business growth?

If you answered **Yes** to any of these questions, then you are unnecessarily living with suboptimal cloud perimeter security conditions.

The good news is that you don't have to settle for any of this. The **Aviatrix Cloud Firewall** solution is designed to address all of these issues so you don't have to compromise.

Aviatrix Cloud Firewall: A Quick Overview

Aviatrix Cloud Firewall delivers a robust solution for managing and securing outbound traffic in both single cloud or distributed multicloud environments. It offers deep visibility, centralized policy enforcement, and advanced traffic engineering, ensuring that egress traffic is both secure and compliant and also optimized for performance and cost-efficiency.

Utilizing Aviatrix Spoke Gateways and NATing capabilities, this solution enables secure, scalable egress management while minimizing operational costs through intelligent resource allocation. Aviatrix SmartGroups further streamline policy management by allowing administrators to logically group resources and consistently apply security rules across diverse cloud environments.

While not required, the solution integrates seamlessly into a transit architecture, complementing Aviatrix Transit Gateways or native solutions like AWS Transit Gateway (TGW) and Azure Virtual WAN. In these setups, Aviatrix enhances native capabilities by providing advanced traffic engineering, unified security policies across all egress points, and comprehensive visibility into outbound traffic.

For enterprises managing complex multicloud architectures, this solution is particularly advantageous. It ensures consistent security policies, reduces egress costs, and improves overall network performance, all while accelerating the deployment of secure cloud environments.

The Top 9 Cloud Perimeter Security Challenges and How You Can Solve Them With Aviatrix

1. Security is inconsistently applied

The Challenge

Security controls need to be applied for both inbound and outbound data. But cloud service providers (CSPs) often handle ingress and egress protocols separately, with a focus on ingress. So if you use cloud-native security tools, you have gaps on the egress side. Additionally, each CSP is different, as is their security, which means you must significantly increase the number of security tools that need to be managed and maintained—potentially even requiring a wide range of skill sets—which also fragments your security controls. In this environment, how can you be sure that your security policies and controls are being enforced fully and consistently?

Aviatrix provides unified cloud security

With Aviatrix unified cloud security, you can apply the same security policies, controls, and architectures consistently for egress communications and across different cloud environments, such as AWS, Azure, Google Cloud, and others, reducing the risk of gaps and inconsistencies. By enforcing a uniform security posture regardless of the cloud provider, you minimize potential vulnerabilities, simplify audits, and maintain compliance across all platforms.

2. Management is fragmented

The Challenge

Complex cloud environments create management challenges. Each cloud provider has an interface for managing, configuring, and monitoring that cloud. Network administrators have multiple consoles to log into, each with its own way of presenting information. All that switching is inefficient, not to mention frustrating. You want your admins focusing on actually managing your clouds, not clicking through tabs to find the right one for the task at hand.

Aviatrix provides single-pane-of-glass management and monitoring

The Aviatrix centralized management console provides a single interface from which you can manage multiple cloud networks. An admin can view, monitor, and manage all cloud egress security easily—for example, AWS VPCs, Azure VNets, and Google Cloud Networks—all from one dashboard. This consolidated control reduces the complexity associated with managing a cloud network to streamline operations.

The Top 9 Cloud Perimeter Security Challenges and How You Can Solve Them With Aviatrix, continued.

3. Compliance is a manual, time-consuming effort

The Challenge

Management isn't the only casualty of fragmentation—there are also governance and compliance repercussions. Even with the compliance tools included with your security and cloud-native solutions, there's no way to confirm that regulatory and governance standards are applied consistently across all of your cloud environments. Any changes need to be applied one by one by one. And audits chew up a lot of time, taking teams away from their core jobs.

Aviatrix provides automated policy enforcement and auditing capabilities

Aviatrix automates this process extensively, ensuring that compliance policies and governance standards are continuously enforced across egress communications for all environments, increasing accuracy while eliminating manual checks and updates. This both aids in maintaining compliance with legal and organizational requirements with minimal manual oversight, and also greatly speeds your ability to adapt to changing standards as needed. Furthermore, central observability greatly simplifies the security policy auditing of estate-wide security enforcement.

4. "Virtualized" hardware appliances are costly

The Challenge

Virtualized hardware appliances were used as a familiar stopgap solution in early cloud infrastructure because they filled technical gaps and minimized the learning curve associated with new cloud technologies. However, because their design is oriented around dedicated hardware, the compute cost of these appliances is high. They also come with traditional licensing models remnant of the static, on-premises era.

Aviatrix delivers cloud operating patterns

Aviatrix is a born-in-the-cloud solution, offering a more effective approach for optimizing cloud operations. Aviatrix follows cloud operating patterns, product lifecycle patterns (upgrades, patching, new feature rollouts), and cloud pricing patterns, which reduces operational friction and costs, improves team performance, and aligns more closely with the inherent benefits of cloud infrastructure.

5. Interruptions are too frequent and take too long to recover from

The Challenge

When your network powers virtually every aspect of your business, you need to make it as resilient as possible. And when interruptions do happen—and they inevitably will no matter how airtight your preventions—you need to keep them as short and unobtrusive as possible. Failover solutions that are cloud-specific can help within a single cloud provider. But when you've got multiple clouds, consistently reliable failover and efficient recovery become difficult challenges to solve.

Aviatrix delivers high availability and rapid disaster recovery

Aviatrix offers cloud-agnostic high availability and disaster recovery capabilities that enable failover mechanisms to work seamlessly across different cloud providers. These automated features provide failover and redundancy, as well as quick recovery options in the event of a failure, outage, or disaster. This helps reduce interruptions and speed recovery times.

The Top 9 Cloud Perimeter Security Challenges and How You Can Solve Them With Aviatrix, continued.

6. Data egress costs are too high

The Challenge

The pricing model for cloud-native NAT gateways typically involves multiple fee types. There is usually a volume component, so the more throughput you have, the higher the monthly cost. This means you're on the hook for increased costs if the cloud-native NAT gateway receives more traffic than expected. Additionally, CSPs charge data egress fees that can quickly mount. Cloud-native NAT gateways don't have mechanisms to selectively block outbound traffic, so you're left with very few options to minimize cost overruns that can strain your budget. In fact, Gartner estimates that data egress charges—which are often based on volume, destination, type of cloud service, and even your subscription level—account for 10–15% of cloud bills. Couldn't all that money be far better spent elsewhere in your cloud operations?

Aviatrix provides a budget-friendly pricing model

Aviatrix offers an "all you can eat" pricing model for traffic processing. Flat hourly billing and no additional cost for throughput will cap your monthly costs and streamline planning and budgeting. And the solution provides the ability to selectively block egress traffic, allowing you to control internet egress charges. In fact, Aviatrix customers routinely save 25% annually on their cloud bills.

7. Overprovisioning is driving up costs

The Challenge

You don't want to pay for cloud resources you aren't using, but keeping your cloud deployments rightsized can be a challenge. There are a lot of cost management tools available, but many don't offer deep integration and may require additional manual adjustments. So, while these tools can certainly help reduce your cloud costs, you may still be missing additional opportunities to save.

Aviatrix provides integrated cost optimization tools

Aviatrix's cost optimization tools track and analyze cloud expenditures, helping you to optimize resource usage and identifying areas where spending can be reduced without compromising performance. This cost optimization is built directly in the Aviatrix networking solution, enabling the delivery of more actionable insights and control compared to third-party products. This enables you to identify and eliminate unused or underutilized resources across all clouds from a single interface for more predictable costs and more effective budget management.

The Top 9 Cloud Perimeter Security Challenges and How You Can Solve Them With Aviatrix, continued.

8. Cloud visibility and monitoring are fragmented

The Challenge

If you can't see what's happening across your cloud network, you can't effectively manage the performance, health, and security of that network. Tools that provide insights within the confines of a single cloud provider help, but they leave you with gaps in visibility which can hide a whole host of problems that can range from minor performance issues to outage-causing conditions.

Aviatrix delivers comprehensive visibility and analytics

Aviatrix offers detailed, holistic monitoring, comprehensive analytics, and visualization tools across all cloud environments, all from a single pane of glass. This enables proactive identification and resolution of issues to improve security, network performance, reliability, and overall user satisfaction.

9. It's hard to scale to accommodate evolving needs and business growth

The Challenge

Change is inevitable. If your cloud network can't keep up with new requirements and increased demand, then it will hold your organization back. But many cloud perimeter security solutions offer limited customization and scalability. This leaves you facing system overhauls that create delays, distractions, and downtime.

Aviatrix provides a flexible framework

Aviatrix's flexible framework can be tailored to specific business requirements and then scaled efficiently as the organization grows. This enables your network infrastructure to truly act as an enabler, supporting business needs over the long term. For example, a tech startup can begin with a small, cost-effective implementation and expand its network capabilities as it scales up without substantial reconfiguration or downtime.

Ready to secure your cloud perimeter without compromise?

Schedule a demo and one of our cloud perimeter security experts will work with you to solve the specific challenges your organization is facing.

SCHEDULE DEMO

ABOUT AVIATRIX

Aviatrix® is the cloud network security company trusted by more than 500 of the world's leading enterprises. As cloud infrastructures become more complex and costly, the Aviatrix Cloud Network Security platform gives companies back the power, control, security, and simplicity they need to modernize their cloud strategies. Aviatrix is the only secure networking solution built specifically for the cloud, that ensures companies are ready for AI and what's next. Combined with the Aviatrix Certified Engineer (ACE) Program, the industry's leading secure multicloud networking certification, Aviatrix unites cloud, networking, and security teams and unlocks greater potential across any cloud.