



Aviatrix Cloud Firewall Fast Facts

KEY BENEFITS

Purpose-Built for Cloud – AWS, Azure, GCP

Embedded and Adaptive Security – Creates a distributed perimeter across the entire cloud network

Comprehensive Control – Gain centralized visibility and control over network traffic across multiple cloud environments

Central Observability – Gain real-time visibility into cloud traffic, anomalies, and policy enforcement across clouds, reducing MTTR and enabling proactive threat response

Increased Attacks Are Causing Enterprises to Rethink Cloud Security

The shift to cloud, multicloud, containers, distributed architectures, and artificial intelligence has fundamentally disrupted legacy security models – introducing unprecedented complexity and risk. The cloud did not just move the perimeter for security – it vaporized it. Hackers are targeting cloud applications at a higher rate and in new and increasingly sophisticated ways, causing businesses to report an uptick in security breaches.

This is causing many businesses to rethink their approach to cloud security to better protect both their customers' data and their mission-critical applications.

\$4.9M

The global average cost of a data breach in 2024: a 10% increase over last year and the highest total ever.

IBM Data Breach Report

Cloud Presents New Challenges for Secure Egress

Unlike a traditional data center, public clouds are designed to give an application quick and easy access to the Internet anywhere it is deployed. This business agility, the primary driver of cloud adoption, makes cloud applications notoriously challenging to protect. Adding to this difficulty is the fact that cloud applications can be deployed in hours or even minutes, making it hard for security teams to keep up. Finally, it's difficult for security teams to implement a new approach to egress security without rearchitecting the network, the application, or both.

The Challenge of Cloud-Native NAT Gateways

First-party solutions like cloud-native NAT gateways give DevOps teams the speed and agility they need, as they are simple to manage and quick to deploy. This makes them popular for agile applications and non-production workloads.

However, in addition to being expensive, cloud-native NAT solutions do not offer application visibility or threat detection. Without embedded security, cloud applications can communicate with malicious endpoints and transmit your data out to the Internet, and you would never know it.

Despite the widespread adoption of cloud-native firewalls, a **2025 survey** showed that two out of three enterprises still struggle to integrate these tools effectively within their broader security stack – exposing dangerous security gaps.

The ideal solution for securing egress communications in the cloud needs to provide enterprise-class security and threat detection with a simple-to-deploy, manage, and scale solution that enables agile frameworks. It should also embed security into the entire network by default without disrupting or impacting your existing architecture.

2/3

**of enterprises
struggle to
integrate
cloud-native
firewalls within
their broader
security stack**

– Aviatrix State of Cloud
Network Security 2025

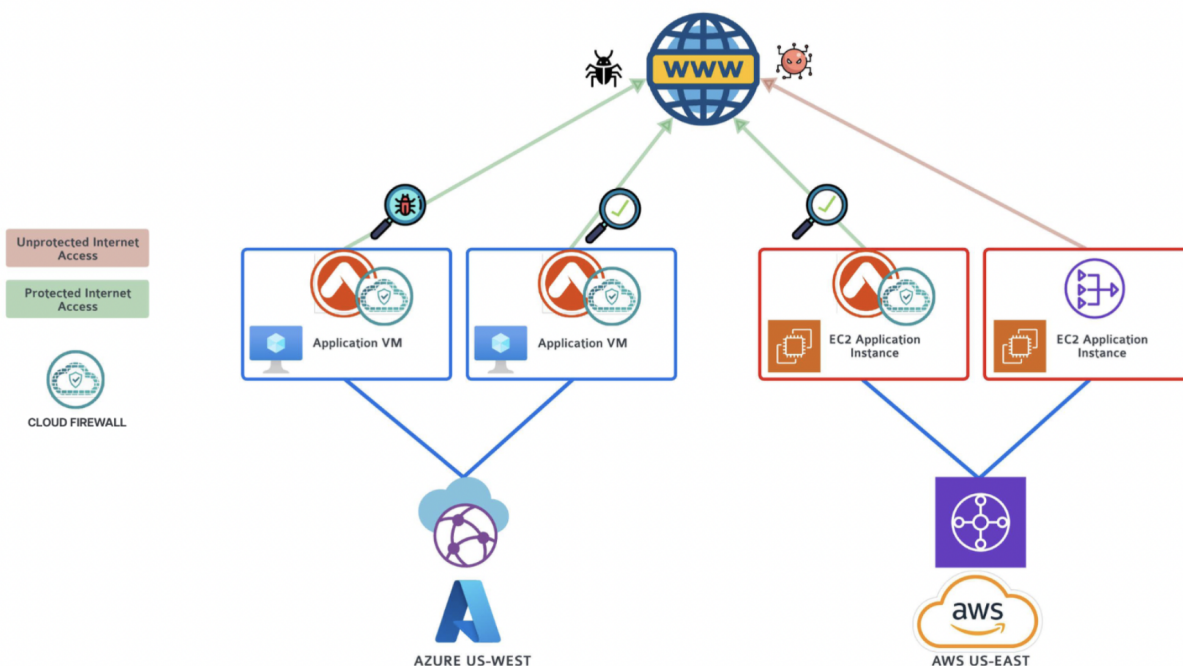
The Solution: Aviatrix Cloud Firewall

Aviatrix Cloud Native Security Fabric (CNSF) redefines network security for the cloud. In the digital age when the traditional network perimeter has vaporized, leaving thousands of micro-perimeters and a huge attack surface, CNSF fortifies network defenses with zero-trust design principles.

Aviatrix Cloud Firewall, part of Aviatrix CNSF, provides visibility and centralized control over Internet-bound traffic, across AWS, Azure, and GCP. It embeds deep application visibility, geo-blocking, and industry-leading threat detection throughout your entire cloud network, creating a distributed perimeter around all your lines of business.

Aviatrix Cloud Firewall is an agile solution that leverages automation and cloud-native orchestration to enable rapid deployment, be it at a global scale, a single region, or just one application at a time.

Most importantly, Aviatrix Cloud Firewall protects your cloud applications where it matters most – anywhere and everywhere they face the Internet in cloud. No complex routing, castle-and-moat architecture, or traffic hair-pinning required. This gives security teams and application owners the complete protection and peace of mind required to build and scale business-critical applications in the cloud.



To see Aviatrix Cloud Firewall in action,
visit [Aviatrix.com](https://aviatrix.com) or [request a demo](#) today.

Request 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 multcloud networking certification, Aviatrix unifies cloud, networking, and security teams and unlocks greater potential across any cloud.