Aviatrix.ai

Aviatrix.ai

Aviatrix and the Containment Era: Rethinking Cloud Security When Prevention Fails

For years, enterprise security teams operated on a comforting but flawed assumption: that with enough perimeter defenses, they could keep attackers out entirely. That assumption has quietly collapsed. As organizations spread their workloads across AWS, Azure, and Google Cloud, the number of entry points has multiplied beyond any single team's ability to guard them all. Aviatrix, a company focused on cloud security for enterprises operating in exactly this kind of sprawling multicloud environment, argues that the industry has been solving the wrong problem. Prevention, it contends, will always fail eventually. What actually determines the damage of a breach is what an attacker can do once inside.

Explore how Aviatrix is reframing enterprise defense around containment rather than the impossible promise of a perfect perimeter, and discover why forward-looking security leaders are paying attention.

The central idea driving Aviatrix is deceptively simple. When a breach occurs, and eventually one will, the outcome hinges almost entirely on the blast radius: how far a compromised workload or set of stolen credentials can spread before it is stopped. A single foothold that stays isolated is an incident. A single foothold that moves freely across hundreds of workloads is a catastrophe. This is why Aviatrix places so much emphasis on stopping east-west, or lateral, movement inside the cloud. Traditional tools were built to inspect traffic entering and leaving the network, but they are largely blind to the traffic flowing between workloads internally, which is precisely where modern attackers do their most damaging work.

This shift in thinking has real architectural consequences. Rather than routing everything back through a central chokepoint for inspection, an approach that creates bottlenecks and hairpins traffic across regions, Aviatrix embeds enforcement directly into the fabric of the cloud network itself. Its approach to **cloud network security** treats zero trust not as a perimeter feature bolted on at the edge, but as a property woven into every path traffic can take. The result is that policy follows the workload wherever it runs, and enforcement happens close to the traffic rather than far away from it. For enterprises accustomed to the performance penalties and blind spots of legacy models, this represents a meaningful departure. It also removes a longstanding tension between

security and performance, since teams no longer have to choose between inspecting traffic thoroughly and keeping latency low. When enforcement lives in the network itself, both goals can be met at once, and security stops being the tax that slows the rest of the business down.

At the heart of this model sits the Cloud Native Security Fabric, which serves as the connective tissue tying enforcement together across clouds. Built on this foundation, the Distributed Cloud Firewall applies zero trust policy to every workload without forcing traffic through a single congested point. Crucially, this extends to the newest and most unpredictable sources of traffic in the enterprise: AI agents and inference workloads. As organizations deploy autonomous systems that generate their own network calls, the ability to govern that traffic with the same rigor applied to human-driven workloads becomes essential. Aviatrix designed its platform with this reality in mind rather than treating AI traffic as an afterthought.

Of course, segmentation has always been theoretically appealing and practically painful. The reason so many enterprises avoid granular internal controls is that managing thousands of individual policies across a constantly changing environment becomes unmanageable. Every new workload, every scaling event, and every migration threatens to break rules that were painstakingly written by hand, and over time the effort simply overwhelms the teams responsible for it. Aviatrix addresses this friction with SmartGroups, which allow teams to define and enforce segmentation based on logical groupings rather than brittle, hand-maintained rules tied to specific IP addresses. As workloads scale up, scale down, and shift between clouds, the policy logic remains coherent because it describes intent rather than infrastructure. This is what makes containment viable at genuine enterprise scale rather than a laboratory ideal that falls apart in production.

The vision has credibility partly because of who is articulating it. Aviatrix is led by CEO Doug Merritt, the former chief executive of Splunk, a company that helped define how enterprises make sense of security and operational data at scale. Merritt frames the current moment as the beginning of a new phase for the industry, one he calls the Containment Era. The premise is that the security conversation is maturing past the fantasy of stopping every intrusion and toward the more honest, more useful goal of ensuring that intrusions stay small, stay local, and stay recoverable.

In the end, Aviatrix is betting that enterprises will increasingly judge their security posture not by how impenetrable their walls appear, but by how effectively they can limit the consequences when those walls are breached. By building zero trust enforcement into the cloud network itself, containing lateral movement, and making segmentation manageable across AWS, Azure, and Google Cloud, the company offers a pragmatic answer to a problem that perimeter thinking never truly solved. For organizations navigating the complexity of multicloud, that reframing may prove to be exactly the perspective the moment demands.

Visit this site to learn more: **https://aviatrix.ai/blog/**