AVIATRIX

FAST FACTS

Aviatrix Kubernetes Firewall

"This solution seamlessly integrates enterprise-grade security into Kubernetes, enabling businesses to scale confidently across hybrid and multicloud environments. Automating governance and unifying visibility helps enterprises reduce complexity, ensure compliance, and drive innovation for enterprises."

David Linthicum, internationally known cloud computing expert, analyst, author, and speaker

Aviatrix Kubernetes Firewall provides enterprises with a **cloud-native**, **scalable**, and **centralized** approach to Kubernetes security by addressing gaps left by traditional Container Network Interfaces (CNIs) and service meshes.

The **Aviatrix Kubernetes Firewall** solution extends Aviatrix's Distributed Cloud Firewall capabilities to Kubernetes environments, providing comprehensive security and networking solutions across multi-cluster and multi-cloud deployments. It addresses the limitations of traditional Kubernetes security tools by offering identity-based segmentation, advanced NAT functionalities, and unified security policies for both containerized and VM-based workloads.

KEY BENEFITS

Operational Efficiency	Consolidates security policies across diverse environments, reducing manual configurations and operational overhead.
Accelerated Adoption	Empowers security teams to match the agility of DevOps, enabling faster, secure cloud and Kubernetes deployments.
Enhanced Security & Compliance	Unifies security policies across clusters and clouds, automating enforcement to reduce compliance risks.
Secure Connectivity	Resolves IP conflicts and connectivity challenges, facilitating seamless communication between Kubernetes clusters and legacy systems.

The Challenges of Traditional Kubernetes Security

Traditional Kubernetes security solutions struggle to scale across multiple clusters and hybrid cloud environments. Traditional IP-based security models fail in dynamic Kubernetes deployments, service meshes lack robust egress control, and enterprises face operational complexity securing both containerized and VM workloads. These gaps create security vulnerabilities, compliance risks, and increased management overhead.

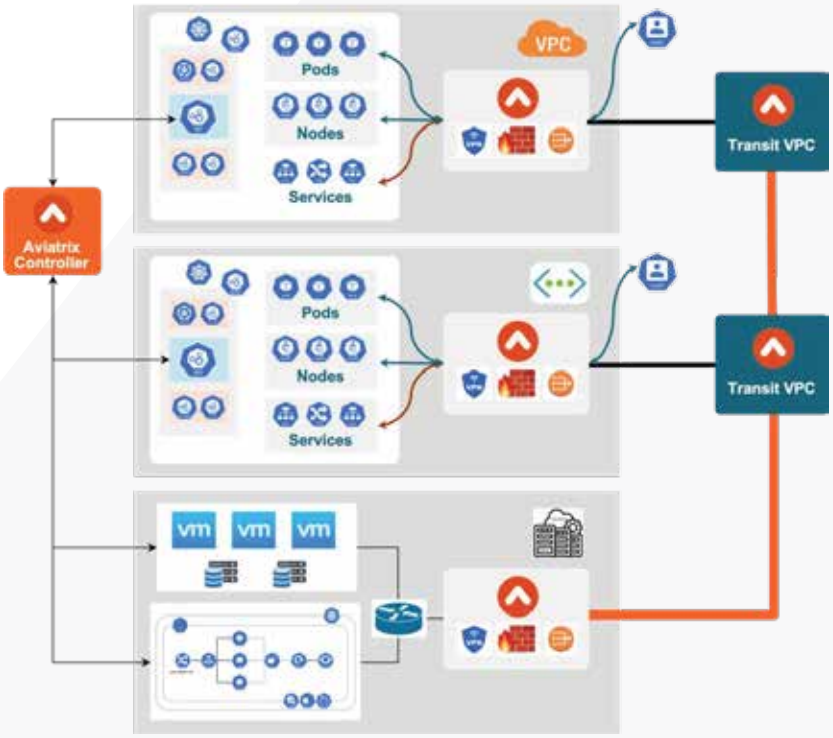
The Opportunity for a Cloud-Native Solution

Enterprises need a unified, scalable approach to Kubernetes and IaaS security that integrates seamlessly across cloud and on-prem environments. By leveraging identity-based segmentation, centralized policy management, and advanced networking capabilities, organizations can simplify security operations, enhance visibility, and ensure compliance—while accelerating cloud-native adoption without security bottlenecks.

THE SOLUTION

Secure Kubernetes at Scale

Aviatrix Kubernetes Firewall extends enterprise-grade security beyond individual clusters, delivering identity-aware protection, multi-cloud visibility, and seamless VM integration. With Advanced NAT for IP management, automated policy enforcement, and egress traffic control, Aviatrix simplifies Kubernetes security, bridging the gap to IaaS workloads, while reducing risk and operational complexity—ensuring enterprises can secure Kubernetes at scale.



KEY FEATURES

- **Granular Identity-Based Security:** Enforces policies using Kubernetes-native identities such as pods, namespaces, and services, moving beyond traditional IP-based security models.
- **Hybrid and Multi-Cloud Visibility:** Offers full visibility into Kubernetes traffic across various cloud environments, facilitating deep observability and real-time policy enforcement.
- **Seamless Integration with VM Security:** Unifies security policies across containerized and legacy VM workloads, ensuring consistent policy application and communication.
- **Egress Traffic Control and Compliance:** Implements policy-based egress filtering to regulate outbound traffic, aiding in compliance with standards like PCI-DSS, HIPAA, and SOC 2.
- **Automated Policy Management:** Provides a centralized control plane for defining, managing, and enforcing policies across multiple clusters and clouds, reducing complexity.
- **KRM-Based Network Segmentation:** Utilizes Kubernetes Resource Model constructs to define and enforce segmentation policies, integrating security into Kubernetes manifests and supporting GitOps workflows.

Scaling Kubernetes Security with Confidence

Aviatrix Kubernetes Firewall offers a scalable, cloud-agnostic solution that extends security beyond individual clusters, unifying policies across containerized and VM-based workloads. By simplifying security management and enhancing compliance, it enables enterprises to securely deploy and manage Kubernetes environments at scale.

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.