AVIATRIX®

FAST FACTS

The AI Security Paradox: Fast Facts on Protecting AI While AI Protects You

The AI Security Challenge

- Security FOR AI– Protecting AI agents and LLMs from hacks and misuse
- AI FOR Security– Using AI to enhance network security through automation and threat detection

Key AI Security Risks

Agent Hijacking– Threat actors can compromise AI agents with access to sensitive data

Data Poisoning– LLM training data can be manipulated to control outputs

Agent Collusion– Multiple AI agents can work together to evade security

Shadow AI– Employees using unsecured LLMs with confidential company data

The Security Gap

95% of organizations use AI/ML for threat detection BUT 63% lack AI governance policies.

AVIATRIX

FAST FACTS

Security FOR AI Protection:

- **Ingress/Egress Filtering** – Inspects incoming traffic for threats and outgoing traffic to prevent data exfiltration
- **Identity-Based Workloads** – Security based on workload vs. ephemeral IP addresses
- **Network Segmentation** – Limits blast radius by isolating system access
- **Policy Enforcement** – Consistent, zero-trust policies across all environments
- **Complete Visibility** – Inline monitoring of all traffic types, including east-west
- **Infrastructure as Code** – Terraform integration for security-first architectures

AI FOR Security Enhancements:

- **Microsoft Secure Network Supervisor with Microsoft Copilot for Security Integration** – AI-powered VPN troubleshooting and remediation
- **Wiz Partnership** – Automated policy enforcement based on AI threat detection
- **Explainable AI (XAI)** – AI-driven insights for informed network decisions

Key Benefits

- ☑ Zero trust principles for AI workloads
- ☑ Prevents lateral movement within networks
- ☑ Closes security loopholes that autonomous agents exploit
- ☑ Scales securely with AI innovation

Ready to secure your AI workloads?
Learn how CNSF protects your network in the age of AI

Aviatrix Cloud Native Security Fabric delivers runtime security and enforcement, closing blind spots so you can scale without compromise.

About Aviatrix

For enterprises struggling to secure cloud workloads, Aviatrix® offers a single solution for pervasive cloud security. Where current cybersecurity approaches focus on securing entry points to a trusted space, Aviatrix Cloud Native Security Fabric (CNSF) delivers runtime security and enforcement within the cloud application infrastructure itself – closing gaps between existing solutions and helping organizations regain visibility and control. Aviatrix ensures security, cloud, and networking teams are empowering developer velocity, AI, serverless, and what's next. For more information, visit www.aviatrix.ai.