Accelerate the Mission with Zero Trust Secure AI Access to the Edge

Andrew Whelchel
Senior Solution Engineer – Federal
Saviynt

Speed is essential to enabling mission delivery. Artificial intelligence (AI) is a modern force multiplier for the digital-enabled joint force. AI enhances the warfighter through AI models running in secure cloud structures and by running in hybrid locations enabled for model execution and data analytics-based model adaptation at hybrid edge environments.

For speed of safe access to both AI model applications and AI data analytics, secure AI access methods enable this needed speed and agility. These secure AI access methods provide rapid data access and reduce the cyber threat risk needed to move at the speed of the mission. The key to enabling and unlocking these capabilities for AI at the edge (and in the secure cloud) is identity access and matching identity to the resources associated with the AI access. When AI access binds to identity, this enables agility of AI resources from cloud to edge while maintaining security and risk reduction throughout the system.

This session highlights several key AI access to edge capabilities including:

- Understanding where the risk is (even if undiscovered) and where it will be
- Leverage AI informed awareness for faster decision actions and reduced risk decisions using Zero Trust and ICAM
- Integrate ICAM in Zero Trust Architecture for Secure AI Access for data access and model integration at the edge