Wednesday, August 17, 2022
12:30 PM – 12:50 PM
Accelerate the Mission with the Unified Network and Zero Trust Identity Access

Andrew Whelchel
Senior Solution Engineer - Federal
Saviynt

Abstract:
The modern operational theater operates in a contested joint environment. In this environment speed and security of access across the unified network mean the difference in operational success. When fully leveraged, the unified network enables new forms of maneuver across the joint environment. To assure success, rapid access to data across the cloud and edge to the unit enable maximum agility for the commander, leader, and soldier to operate with reliability of communications and engage the data for the multi-domain enabled mission. As a part of this capability, identity least-privilege access to attributes enables rapid and secure access to these resources while minimizing risks to operate at full speed of the mission.

The unified network employed with cloud-enabled identity access addresses key challenges found in accessing data across multi-domain data fabrics from command post to contested edge. Some of these challenges include how to conduct data access validation in a contested environment, how to sustain reliable AI/ML data access in a potentially disconnected environment, and disengaging data access if needed for data disposition.

To address these challenges, cloud-enabled identity access and identity security controls combine to provide needed agility and security for data access across multiple domain operations. Delivering on these challenges requires a cloud-enabled identity access capability set that is accessible from operations planning to edge theater operations.

The cloud-enabled identity access for the unified network innovative approach addresses these challenges by enabling the following for the mission:

- Provide data access authorization capability across the unified network from AI/ML and dynamic sources that can drive rapid data access decisions in a joint contested environment. This data access operates with the option of disconnected or connected environments and maintains an identity chain of access audit trail needed for cyber assurance of the mission.
- Provide a zero-trust approach for access by leveraging governance requests and risk reviews of data attributes (ABAC attributes) in the unified network and use as authorization for access to abstracted data and data products for the mission.
- Create secure data access path for operational integration of data analytics across data fabrics (e.g. secured, MPE, et al.) using identity access for common data presentation from the command post to edge field environment (such as CMFF).

Rapid and secure data access via a unified network with cloud-based identity access is necessary for the future success of the execution of information warfare for the joint multi-domain mission. The capabilities described here would leverage all the data security functions and identity controls to provide rapid and agile access to the unified network data to succeed in the joint multi-domain mission.