Wednesday, June 3

2:50 pm – 3:10 pm

Built for Disruption: Zero Trust in Contested and Disconnected Operations

Chris Betz

Federal CTO, Omnissa Federal

Omnissa

Abstract:

Zero Trust strategies are often designed around persistent connectivity, assuming continuous access to centralized policy engines, cloud control planes, and real-time data exchange. Military and government operations rarely have that advantage. In contested, degraded, or fully disconnected environments, those assumptions break down, creating gaps in enforcement, visibility, and control at the exact moment they are needed most.

This session focuses on how Zero Trust must be implemented to operate through disruption, not around it. When connectivity is limited or unavailable, security decisions cannot rely on constant reach-back to centralized infrastructure. Instead, trust must be continuously evaluated and enforced locally using device posture, identity context, and session state—ensuring security controls remain intact at the tactical edge.

Omnissa will outline a practical, operational approach to extending Zero Trust into these environments by embedding policy enforcement directly into endpoints, access workflows, and controlled execution environments. This allows DoD components to maintain least-privilege access, reduce credential exposure, and limit lateral movement—even when operating offline. When connectivity is restored, telemetry and policy state are synchronized to support auditability, compliance, and broader situational awareness.

Attendees will learn how to:

---Shift enforcement from network-dependent controls to device, identity, and session-based decision points

---Maintain policy-driven access and compliance posture during intermittent or disconnected operations

---Reduce reliance on static credentials and centralized infrastructure in contested environments

---Preserve mission continuity and security assurance without requiring persistent connectivity

This session reframes Zero Trust as an operational capability built for the realities of modern defense, designed to function in denied, degraded, intermittent, and limited (DDIL) environments, while delivering a cloud-operating model across on-prem and fully disconnected deployments.