Aligning ICAM, the Executive Order & Zero Trust for the Defense Department

Josh Brodbent
RVP, Public Sector Solutions Engineering
BeyondTrust

In our rapidly changing digital world, agencies must evolve security strategies. A goal of Zero Trust is to create a security and network architecture that is dynamic, adaptable, and protected. The Executive Order on Cybersecurity has moved the term "Zero Trust" from a buzzword to a much-needed mindset shift in how we secure agency data and systems. Agencies must leverage Zero Trust principals to never trust, always verify, and only allow access when contextual parameters are met.

Identity sits at the heart of Zero Trust. In a perimeter-less world, agencies must think through ways to prove an identity for access to stop adversaries from getting in and ultimately from moving laterally within an environment. Leveraging ICAM and robust identity security strategies enables agencies to move from a network-based approach to a data centric approach to defending systems.

Join BeyondTrust and government security experts for a panel discussion to understand:

- Why Privileged Access Management (PAM) is essential to major DoD initiatives like ICAM, Thunderdome, and Zero Trust
- How ICAM supports the Executive Order
- The Defense Department's outlook on data centric security and defending agency systems
- The path to secure modernization using Least Privilege