Control the Who, What, When, Why & Where of Mission Partner Environment Access

James Ebeler
Chief Technology Officer
Three Wire Systems

Andy Shook
Senior Solutions Engineer
BeyondTrust

Zero trust is about knowing who is doing what within your network and ensuring that in the event of anomalous activity, you can control and limit threats to your network. Applying the granularity of Privileged Access Management (PAM) to achieve zero trust objectives ensures all access is appropriate, managed, and documented, regardless of how the perimeter has been redefined. To stay agile, Defense agencies must implement PAM to enable Zero Trust, JADC2, ICAM and other mission critical agency initiatives.

Join this technical session to understand how PAM:

• Inventories all privileged assets to eliminate blind spots, spotlight shadow IT, and control access points for separation of control and data planes.

• Applies least privilege controls for every identity, account, and secret—human, application, machine, employee, vendor, etc.

• Enforces adaptive and just-in-time access controls based on context in real-time.

• Implements segmentation and microsegmentation to isolate assets, resources, and users to prevent lateral movement.

• Enforces credential security best practices for all privileged password types—whether for humans, machines, employees, or vendors.

• Secures remote access with granular least privilege and adaptive capabilities well beyond that of VPNs, RDP, SSH, HTTPS, and other commonly used technologies.

• Proxies access to control planes (cloud, virtual, DevOps) and critical applications by enforcing network segmentation.

• Monitors, manages, and audits every privileged session that touches the enterprise for appropriate user behavior.