CyberCloak™ Solution Mapping for DoW Zero Trust Operational Technology Framework

Blue Ridge Networks' CyberCloak cybersecurity solution maps well with DoW OT Zero Trust objectives[1]. CyberCloak's aligned capabilities include deterministic hardware-enforced isolation, authenticated conduits, cryptographically controlled access, secure remote authenticated access, and elimination of routable adjacency. These capabilities produce the following outcomes **Zero Trust micro-segmentation**, **deny-by-default, secure zones between Enterprise IT and OT Environments**, and **protection of data-in-transit** as outlined in the DoW OT Activity tables.

The DoW document emphasizes preventing lateral movement, controlling all OT entry points, enforcing credentialed communications, and separating Operational and Process Control layers. CyberCloak's immutable overlay architecture, hardware trust anchors, non-routable pathways, and deterministic segmentation achieve these outcomes without dependence on traditional firewalls, ACLs, or SDN complexity.

DoW OT Zero Trust & CyberCloak

Mapping across the five Zero Trust pillars used in DoW OT guidance is summarized below.

User Pillar (Identity, Access Control, Authentication)

Relevant DoW Activities

- 1.2.2.OT – Role-Based Dynamic Access for OT Environments – Requires strict role-based enforcement and dynamic access control.
- 1.3.1.OT / 1.8.1.OT – Authentication & Session Enforcement – Requires MFA and session-based authentication.
- 1.7.1.OT – Deny by Default Policy for Users – Remove unnecessary permissions.

Hubs (BorderGuard), Gateways (RemoteLink), and Agents (EdgeGuard) secure remote access enforces identity-linked cryptographic trust between nodes, zones, and conduits.
Capabilities include:

- Machine-to-machine identity binding (similar to "NPE Credentialing" in 2.1.3.OT).
- Strict deny-by-default access: a RemoteLink gateway or EdgeGuard agent can only communicate through policy-driven encrypted conduits to its assigned BorderGuard hub.
- No open ports or routable attack surface.
- Independent of AD, RADIUS, TACACS—aligns with OT need for deterministic availability even if enterprise identity services fail.
- Software engineered to be agilely integrated with off-the-shelf or specialized hardware hosts.

Strength: CyberCloak provides deterministic identity-based access for machines, which allows OT operators to meet user and NPE-based Zero Trust outcomes without introducing additional attack paths or dependencies on enterprise IAM inside OT zones.

Device Pillar (NPE Management, Certificates, Deny-by-Default)

Relevant DoW Activities

- 2.1.1.OT – Inventory of NPEs
- 2.1.2.OT – NPE Certificate Management
- 2.4.1.OT – NPE Deny-by-Default – Block unauthorized access.
- 2.7.1.OT – EDR/Monitoring Requirements.

Blue Ridge's CyberCloak contributes to device Zero Trust by the following:

- Treating each Hub (BorderGuard) and Gateway (RemoteLink) or Agent (EdgeGuard) as a known, cryptographically authenticated and validated non-person entity (NPE).
- Supporting Data Privacy Facility (DPF) protocol communication and identity management in a closed network model with no broadcast, discovery, or lateral communication.
- Supporting hardware-based roots of trust (TPM, chip-based, other).
- Enforcing absolute deny-by-default at the hardware level; a RemoteLink cannot communicate with anything except its approved BorderGuard hub(s) and resilient/redundant pool(s).
- Dramatically reducing the EDR surface: EDR still required per DoW guidance, but CyberCloak reduces the reachable attack surface to near-zero.

Strength: CyberCloak provides physical and cryptographically constrained conduits that inherently satisfy 2.4.1.OT and reduce the complexity of NPE authorization—no unmanaged interfaces, no local VLAN misconfigurations, and no unexpected routable connections.

Applications & Workloads Pillar

Relevant DoW Activities

- 3.4.1–3.4.4.OT – Access Control Enforcement (ABAC) – Require digital policy enforcement for applications.
- 3.1.1.OT Application Inventory, 3.1.2.OT Application Control.

CyberCloak is not an application-layer security tool. It creates a cryptographically sealed delivery fabric through the Data Privacy Facility (DPF), which only approved applications can communicate between layers. This supports the following:

- Enforcement of least-privilege application connectivity
- Prevention of unauthorized application flows
- Guaranteed routing of OT application traffic only through protected conduits
- Agnostic to network transport and application protocols or management plane interfaces to authenticate sessions or maintain cryptographic separation.

Strength: CyberCloak simplifies Zero Trust workload security by eliminating the possibility of unexpected application traffic paths, which is critical for legacy OT systems that cannot support ABAC/RBAC natively.

Data Pillar (DLP, DRM, Data Tagging, Secure Transport)

Relevant DoW Activities

- 4.4.6.OT – Database Monitoring & Protection
- 4.5.3–4.5.4.OT – DRM Response & Data Encryption
- 5.4.3.OT – Protect OT Data in Transit – Must encrypt data in transit per policy.

Blue Ridge Networks' CyberCloak overlay provides the following:

- Policy-driven and configured cryptographic key pairs with no third party or PKI dependencies.
- End-to-end AES-256 encrypted tunnels for all OT data flows (exceeds data-in-transit mandates under 5.4.3.OT).
- Topology and infrastructure "cloaking" and integrity protection that prevents unauthorized data interception or replay.
- Isolation of data flows from enterprise IT, ensuring only sanctioned flows reach the OT boundary.

Strength: CyberCloak satisfies the data-in-transit protection requirement without altering OT protocols, including non-secure industrial protocols such as DNP3 or Modbus.

Network / Micro-Segmentation Pillar

Relevant DoW Activities

- 5.3.1.OT – Management and Data Plane Segmentation
- 5.4.1–5.4.2.OT – Micro-Segmentation & Device-Level Segmentation
- 5.2.2.OT – Programmable Infrastructure
- 2.2.1.OT – Connection Policy Enforcement

These are among the most critical Zero Trust activities for OT.

CyberCloak provides the following:

- Cryptographically enforced segmentation independent of VLANs, firewalls, or SDN policies.
- Micro-segmentation implemented as explicit conduits, not logical firewall rules.
- Separate conduits for Enterprise IT → Operational Layer → Process Control Layer, directly reflecting the layered architecture in the Dow OT diagram (p. 3).

Strength: CyberCloak enables true Zero Trust segmentation even where legacy hardware, unsupported controllers, or "flat" OT networks exist. It does not require changes to routers, switches, or PLC networks.

Mapping to the DoD CSRA 5.0 Architecture

The CSRA 5.0 defines Enterprise IT, Operational IT, and OT Process Control layers.

Blue Ridge maps into the CSRA as follows:

Hub

- BorderGuard (BG) appliances can be placed in the Enterprise IT layer, near the Demilitarization Zone (DMZ), or secure interconnect zones.

- CyberCloak Cloud (Cloud-Hosted BorderGuard)

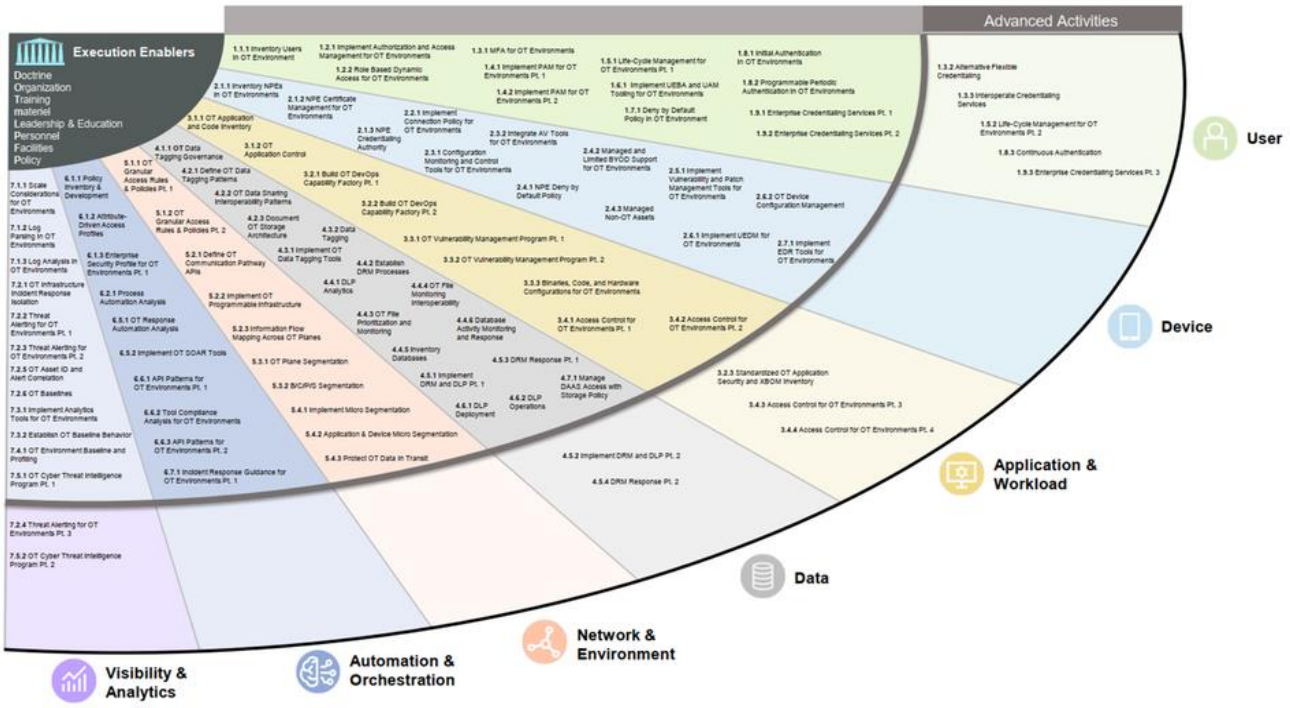
Spoke

- RemoteLink (RL) devices can be placed:
  - In the Operational Layer for SCADA servers, HMIs, historians
  - In the Process Control Layer for PLC networks, safety systems, engineering workstations
- RemoteLink firmware can be integrated into host or chip-based systems.
- EdgeGuard software agents can be installed in computing devices.

Mesh

- Hubs and Spokes can be physically or logically configured to create distributed mesh operations.

These attributes address the CSRA requirement that all OT communication should traverse controlled, authenticated decision points.



Zero Trust Fan Chart for Operational Technologies[1]
More guidance for Zero Trust Activities and Outcomes can be found at www.dowcio.war.gov.

CyberCloak Strengths for DoW Zero Trust OT

Non-Routable, "Cloaked" Attack Surface

DoW guidance repeatedly emphasizes limiting reachable surfaces, preventing lateral movement, and enforcing segmentation. CyberCloak overlay creates a far stronger segmentation model than firewalls or VLANs.

- No IP routability except through the hub
- No broadcast domains, ARP exposure, or port scans
- Cryptographically isolated, deterministic paths

Hardware-Enforced Trust Boundaries

DoW stresses the need for isolation between Enterprise IT and OT and controlled conduits (e.g., 5.3.1.OT, 5.4.1.OT). CyberCloak enforces a physical anchor for Zero Trust policy enforcement.

- Physical termination points for all OT-bound connectivity
- Immutable security controls

Legacy OT Compatibility

A core concern of DoW OT ZT (highlighted heavily in the introduction, pp. 1–3) is that OT devices cannot be patched, upgraded, or modified easily. CyberCloak achieves ZT outcomes without jeopardizing availability or safety, one of the biggest challenges highlighted in the DoW OT document.

- No protocol changes
- No agent installation
- No modifications to PLCs or SCADA servers

Summary

In summary, Blue Ridge Networks' CyberCloak zero trust cybersecurity solution maps along 5 pillars within the DoW's Zero Trust for Operational Technology Activities and Outcomes. The solution aligns to the targeted activities and outcomes in the User, Device, Applications and Workloads, Data, and Network and Environment pillars. CyberCloak delivers a proven, autonomous security solution that strengthens network resilience, simplifies integration, and delivers zero trust preemptive cyber protection for critical assets and operations.

More information on CyberCloak can be found at www.blueridgenetworks.com.

Note: 1. The DoW Zero Trust for Operational Technology Activities and Outcomes guidance can be found at dowcio.war.gov.

1-800-704-5234
sales@blueridgenetworks.com
BlueRidgeNetworks.com