OWL Cyber Defense

Cross Domain Solutions & Zero Trust:

Reinforcing Cybersecurity at the Tactical Edge

As cyber threats continue to evolve in complexity and sophistication,

the U.S. government, particularly within the Department of Defense (DoD), has increasingly embraced **Zero Trust Architectures (ZTA)**. The Zero Trust model, based on the principle of "never trust, always verify," challenges the traditional perimeter-based security approach by assuming that threats can come from both inside and outside the network. This paradigm shift is crucial for safeguarding national security, especially as military operations become more dependent on digital networks and real-time data.

However, while Zero Trust provides a robust framework for securing these operations, the ability to work effectively across different security domains requires additional reinforcement. This is where Cross Domain Solutions (CDSs) become indispensable. These technologies, particularly when embedded in weapons and other assets at the tactical edge, enable warfighters to gather intelligence rapidly and react swiftly—capabilities that are critical to military success. Owl Cyber Defense, as a trusted industry leader, is perfectly positioned to support these efforts, with cutting-edge solutions like **V2CDS** making cross-domain operations even more secure and effective.

ZERO TRUST PILLARS

Pillar	Description
User	Involves focus on user identification, authentication, and access control policies which verify user attempts connecting to the network using dynamic and contextual data analysis.
Device	Performs "systems of record" validation of user-controlled and autonomous devices to determine acceptable cybersecurity posture and trustworthiness.
Network	Isolates sensitive resources from being accessed by unauthorized people or things by dynamically defining network access, deploying micro-segmentation techniques, and control network flows while encrypting end-to-end traffic.
Infrastructure	Ensure systems and services within a workload are protected against unintended and unauthorized access, and potential vulnerabilities.
Application	Integrates user, device, and data components to secure access at the application later. Security wraps each workload and compute container to prevent data collection, unauthorized access or tampering with sensitive applications and services.
Data	Involves focus on securing and enforcing access to data based on the data's categorization and classification to isolte the data from everyone except those that need access.
Visibility and Analytics	Provides insight into user and system behavior analytics by observing real-time communications between all Zero Trust components.
Orchestration and Automation	Automates security and newtork operational processes across the ZTA by orchestrating functions between similar and disparate security systems and applications

The Imperative of Cross Domain Solutions in a Zero Trust World

The adoption of Zero Trust within the DoD underscores the importance of rigorous verification and continuous monitoring of all network traffic. In practice, this means that every user, device, and piece of data is treated as a potential threat until proven otherwise. While this approach is effective at securing networks, it poses significant challenges when it comes to the exchange of information across security domains—particularly in environments where classified and unclassified data must be seamlessly integrated.

What is a Cross Domain Solution?

→ A high-assurance controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains

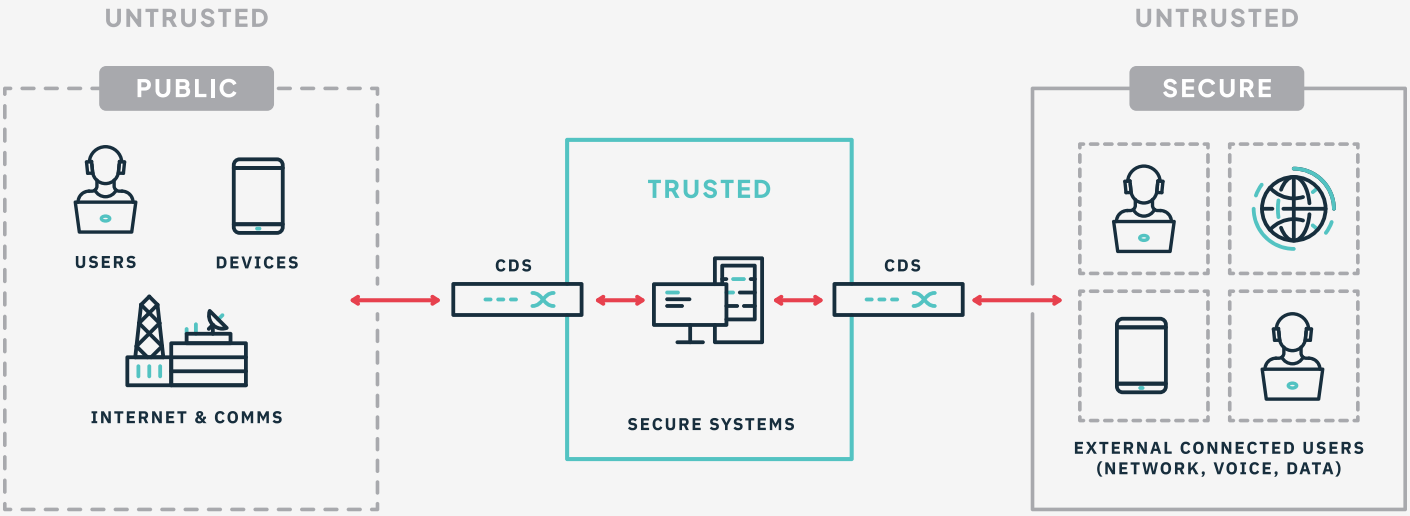
→ Content / Data Filtering–Network / Application Layer

→ Transfer vs. Access Solutions

Cross Domain Solutions: Bridging Security Domains

Cross Domain Solutions (CDS) are designed to securely transfer information between networks of different classification levels.

In a military context, this capability is crucial. Warfighters operating at the tactical edge need access to real-time intelligence that may originate from both classified and unclassified sources. CDS ensures that this information can be securely exchanged without compromising the integrity of sensitive data or exposing critical systems to unauthorized access.



In a Zero Trust environment, CDSs take on an even greater significance. By enforcing stringent access controls, policy-based data filtering, and robust authentication mechanisms, CDSs aligns directly with the core principles of Zero Trust. These solutions ensure that only verified, authorized, and non-malicious data can cross domain boundaries, thereby preventing data leaks and unauthorized access. This is particularly important in scenarios where operational decisions must be made rapidly, and the timely flow of information can mean the difference between mission success and failure.

Strengthening Military Operations & Information Dominance

The integration of CDSs into weapons systems and other military assets at the tactical edge provides warfighters with a strategic advantage.

In modern warfare, the ability to rapidly gather, process, and act on intelligence is critical. CDSs enable this by facilitating secure, real-time data exchange between different security domains. This capability allows commanders to make informed decisions quickly, enhancing the agility and effectiveness of military operations.

Moreover, the deployment of CDSs at the tactical edge reinforces the security of these operations. By ensuring that sensitive data is protected even as it moves between domains, CDSs helps to maintain the integrity of military communications and prevent adversaries from exploiting potential vulnerabilities. This level of security is essential in an environment where cyber threats are not only more frequent but also more sophisticated.

Challenges and Considerations in Zero Trust Implementation

While the integration of CDSs strengthens the security stack in a Zero Trust environment, their implementation is not without challenges.

One of the most significant challenges is ensuring that these technologies are seamlessly integrated into the broader security architecture. This requires careful planning, ongoing management, and a deep understanding of the unique requirements of military operations and the specific needs of each mission environment.

The integration of CDSs into existing military networks is a complex task. These technologies must work in concert with other security tools, such as intrusion detection systems (IDS) and security information and event management (SIEM) platforms, to provide continuous monitoring and threat detection. Any gaps in this integration could leave the network vulnerable to attack, undermining the effectiveness of the Zero Trust framework.

Ensuring that these technologies are scalable and adaptable to the changing needs of military operations is essential for maintaining both security and operational efficiency. This includes avoiding "vendor lock" and allowing the capability for the devices to be adjusted in the field without the need for on-site assistance from the CDS vendor.

Owl Cyber Defense: Leading the Way in Cross-Domain Security

As the DoD and other government agencies continue to refine their Zero Trust architectures, security architecture experts from Owl Cyber Defense have been trusted for over 25 years to assist U.S. Government customers with meeting regulatory requirements associated with their security posture.

With a proven track record of delivering secure, reliable network security solutions, and deep ties to the compute platform industry, Owl is also uniquely positioned to support the complex security needs of military operations at the tactical edge.

Owl solutions are also configurable by the end user and do not require on-site vendor administration to maintain the continued support and integrity of the device.

V2CDS: Bringing Zero Trust to the Tactical Edge

Owl's V2CDS is a prime example of how cross domain solutions are evolving to meet the needs of modern military operations. V2CDS enables secure, validated and filtered video and voice communication across classified and unclassified domains. This capability is particularly important in environments where timely decision-making is critical to mission success. V2CDS has already been deployed on a number of tactical platforms and proven in the field in multiple deployments.

Zero Trust represents a significant advancement in the way government agencies, particularly within the DoD, approach cybersecurity. However, the complexity of modern military operations requires additional reinforcement from technologies like cross domain solutions and data diodes. These tools are essential for ensuring that sensitive information can be securely transferred across domains, protecting critical systems from cyber threats, and supporting the rapid, secure decision-making that is vital to military success.

Owl Cyber Defense, with its industry-leading solutions and deep expertise in cross-domain security, is ideally positioned to support these efforts. As the DoD continues to implement and refine its Zero Trust architecture, the integration of innovative security solutions like V2CDS will be critical in maintaining the integrity and effectiveness of military operations at the tactical edge. To learn more, visit owlcyberdefense.com.