EVERFOX

FREQUENTLY ASKED QUESTIONS

Why Zero Trust Needs a Bridge

Security Across Boundaries

Why Isn't Zero Trust Enough On Its Own?

Zero trust works well within a single network boundary, enforcing least privilege, strong identity, and continuous verification. However, missions today, demand data sharing across agencies, partners, and coalition environments with different trust and classification levels.

That's where zero trust alone breaks down. Cross Domain Solutions (CDS) act as the "bridge" that extends zero trust beyond a single environment, providing policy-enforced, auditable sharing between trusted and less-trusted domains.

Can CDS Filter Traffic for Functional Applications (e.g, identify & filter out XML or JSON files based on templates)?

Yes. CDS applies both syntactic and semantic inspection rules to data flows. For example, it can enforce XML/JSON schema validation, apply pre-defined policy rules, and block non-conforming or malicious data structures. While many use cases are straightforward, some complex or undefined data structures require additional policy design.

How Does CDS Apply to Financial Services?

While CDS has its roots in defence and intelligence, the same principles of secure, policy-enforced data exchange across trust boundaries apply to all critical services and industries.

How Can You Implement CDS and ZTA in Critical Infrastructure with Legacy Systems?

CDS can help bridge the gap between modern Zero Trust Architectures (ZTA) and legacy systems. Where legacy systems are not zero trust compliant, CDS access and transfer controls can compartmentalise them.

This allows you to still access and integrate those systems without making them part of the zero trust environments. In this way, organisations avoid the expense of replacing entire infrastructures, while reducing exposure and maintaining interoperability.

What are the Compute and Management Overheads Associated with Advanced CDS Deployments Across an Extended Enterprise?

The answer is very use case dependent. CDS solutions can be implemented in both hardware and software. Hardware-enforced CDS is deterministic, maintaining predictable performance with low overhead. Software-based CDS is less deterministic, but highly-flexible. The compute and management overhead depends on scale, classification level, and mission requirements.

For deeper guidance, we recommend setting up a meeting with our team to review your operational environment.

How Does CDS Support Coalition Operations Like FVEYS or NATO?

Coalition operations depend on trust, CDS provides a trusted gateway that allows:

- Only the right data, in the right format leaves a national network
- Nations retain sovereign control over what they share
- Transfers are audited and policy-enforced

This makes CDS a critical enabler for FVEYS, NATO, AUKUS, and other coalitions working on the principle of "share more, risk less."

You Spoke of CDS Technologies - Can You Name a Few and What Specifics Are Required When Thinking About Them?

Broadly, CDS technologies fall into two categories:

CDS access, isolates a user from destination networks that cannot be trusted. Allowing them to view and interact with the information, without allowing any data to enter a user's network.

This technology enables multi-mission partner collaboration environments while allowing each partner to maintain a zero trust posture and preserve network sovereignty.

CDS transfer, isolates networks of varying classifications and varying owners from each other. Allowing for the secure transfer of data across networks, such as data streams, files, chat streams, video feeds, and more.

The security and classification policies associated with the data is preserved in transit and the data is inspected, validated, and any potential threats embedded in the data is removed.

What Types of Mission Data Benefit Most From CDS?

CDS is critical wherever sensitive but shareable information exists, such as;

- → Intelligence, Surveillance, and Reconnaissance (ISR) feeds (UAV/drone video, sensor streams)
- → Multi-domain operational data summaries and coalition reporting
- → Critical digital infrastructure data (energy, transport, comms)

In all cases, the mission benefit comes from enabling faster speed to decision while protecting classified networks.

How Does CDS Fit With Digital Modernisation Strategies Like The UK MOD's Integrated Force, or Digital Backbone?

Both strategies emphasise interoperability, data-centric security, and faster speed to decision. CDS directly supports these by:

- → Acting as the secure connective tissue between domains, services, and nations
- → Enforcing policies aligned to zero trust principles
- → Safeguarding ISR data as it flows into decision-making and operational systems

CDS therefore underpins the digital targeting web and the integrated force concepts described in the MOD's Strategic Defence Review.

Do You Have a Roadmap of Future Functionality?

Yes, Everfox continuously evolves its CDS capabilities in line with NATO, FVEYS, and allied requirements.

This includes support for collaboration and chat platforms. For any specific functionality requirements, please reach out to discuss further with a member of the Everfox team.

How Does Everfox CDS Integrate With Other Technologies, Such as Data Platforms or AI/ML Systems, to Support Multi-Domain Operations?

Everfox Cross Domain Solutions are designed to be the trusted foundation layer that enable interoperability between mission technologies.

By acting as a data assurance layer, our CDS makes it possible for governments, defense, and intelligence agencies to safely adopt advanced technologies, such as Palantir, to help make multi-domain, AI-driven operations a reality.

↘ Contact Everfox