Secure Computation Across the Boundary

Adding Secure Computation to the Cross-Domain Ecosystem

August 2026

Kurt Rohloff, Cofounder & CTO

krohloff@dualitytech.com

Executive Summary

Cross-domain solutions move information across security boundaries. They do not provide a means to compute across them. Duality Technologies provides that computation layer through its secure query capability. Secure query allows a high-side analyst to search, resolve, and analyze data held on lower or partner domains. Secure query protects sensitive information in the query itself. It is enabled by Fully Homomorphic Encryption (FHE) and the broader family of privacy-enhancing technologies (PETs). By using the FHE-enabled secure query capabilities, the query, the results, and the analyst's intent are never revealed. This paper refers to the combined configuration as Secure-Collaboration-Enhanced Cross-Domain (SECD) capability. The accredited boundary remains the sole transit and policy enforcement point. Duality provides a governed computation layer above it.

The need for SECD comes from how missions now use data. Joint and coalition operations depend on data that different organizations hold and cannot freely share. Analytics and AI raise the stakes: the most valuable questions span domains that were separated on purpose. Today those questions are answered by moving data, by slow manual release processes, or not at all. SECD closes that gap. Queries and analytics run over data that never moves and is never exposed. The cross-domain boundary is the natural place to anchor this capability, because it is already the accredited path between the domains involved.

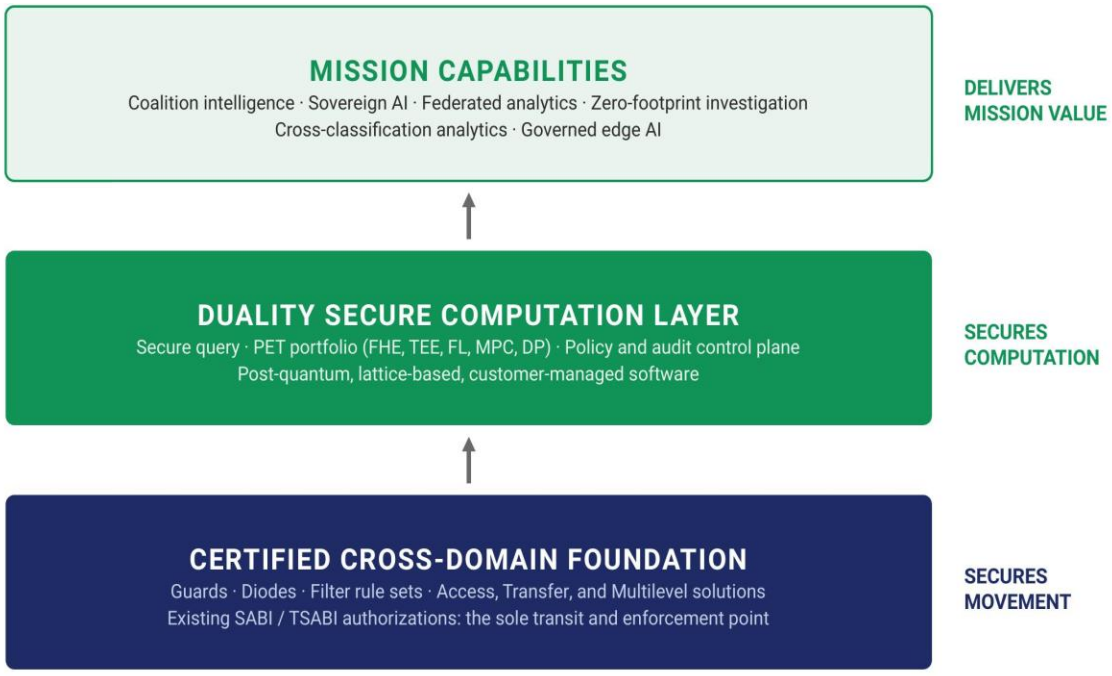

Figure 1. The SECD stack: the accredited boundary secures movement, the Duality layer secures computation, and the combination supports mission capabilities available from neither layer alone.

The paper opens with a brief cross-domain primer based on public NCDSMO material [1][2]. It then describes how secure query complements an accredited boundary and how the accreditation case

relates to publicly stated Raise the Bar principles. A worked example over a commercial Low Earth Orbit (LEO) satellite link shows what the capability changes for the mission. Later sections cover the broader PET portfolio, governance, data-centric security, integration in practice, and how Duality works with the cross-domain ecosystem. The paper closes with ten questions we expect from the community, and public references.

The Value Proposition

Duality's secure query capability, enabled by FHE and operating over certified cross-domain infrastructure, provides the following properties:

- **Automated cross-domain query.** Queries that currently require manual release and disclosure processes execute in an automated manner through the existing boundary, with end-to-end times measured in seconds to minutes.
- **Reduced data movement.** A query and its result are megabyte-scale; bulk transfer of source data is not required. The reduction is material on bandwidth-constrained and intermittent links.
- **Query in place across trust boundaries.** The computation travels to the data, as in federated and data-mesh architectures, but the query and the results remain hidden from the system that holds the data.
- **Confidentiality of data, query, and result.** None appears in plaintext outside the analyst domain: in transit, at rest, or during computation.
- **Need-to-know enforcement.** Query content is not visible to personnel or administrators on the queried side. Authorization and audit records remain available for oversight.
- **Reduced consequence of platform loss.** A lost or captured edge platform holds no plaintext data and no readable record of the queries made against it.
- **Post-quantum protection.** The underlying lattice-based cryptography is consistent with NSA CNSA 2.0 and protects cross-domain flows against harvest-now-decrypt-later collection.
- **Use of existing accreditations.** The certified boundary, its rule sets, and existing SABI/TSABI authorizations remain the sole transit and enforcement point; no new boundary type is introduced.
- **Sovereignty compatibility.** Each participating nation or program retains its own keys, data, and infrastructure while participating in joint analysis.
- **Governance.** Computation policy is enforced cryptographically, and every step is logged and verifiable.
- **Integrator delivery model.** Duality supplies software; integration, accreditation support, and lifecycle sustainment are performed by the integrator.

1. Cross-Domain Solutions: A Brief Primer

Readers inside the cross-domain community can skim this section. It establishes the terminology the rest of the paper uses. The definitions follow public material from the National Cross Domain Strategy and Management Office (NCDSMO), the NSA office that serves as the U.S. Government focal point for cross-domain capabilities [1][2]. Department of Defense cross-domain policy is set out in DoD Instruction 8540.01 [3].

A cross-domain solution (CDS) is a controlled interface between networks operating at different security levels. It enables access to information, or transfer of information, across that divide. The defining property is enforcement. A CDS does not merely connect two networks; it mediates every interaction between them under an accredited policy.

1.1 The NCDSMO taxonomy: Access, Transfer, Multilevel

Public NCDSMO material divides cross-domain solutions into three types [1]. Access solutions let one user reach multiple networks from a single endpoint. No data moves between the networks. Transfer solutions move data between domains through inspection and filtering. Guards and data diodes belong to this class. Multilevel solutions store and process data at multiple classification levels within a single accredited system. This paper concerns primarily Transfer solutions, because computation across a boundary rides on the transfer path.

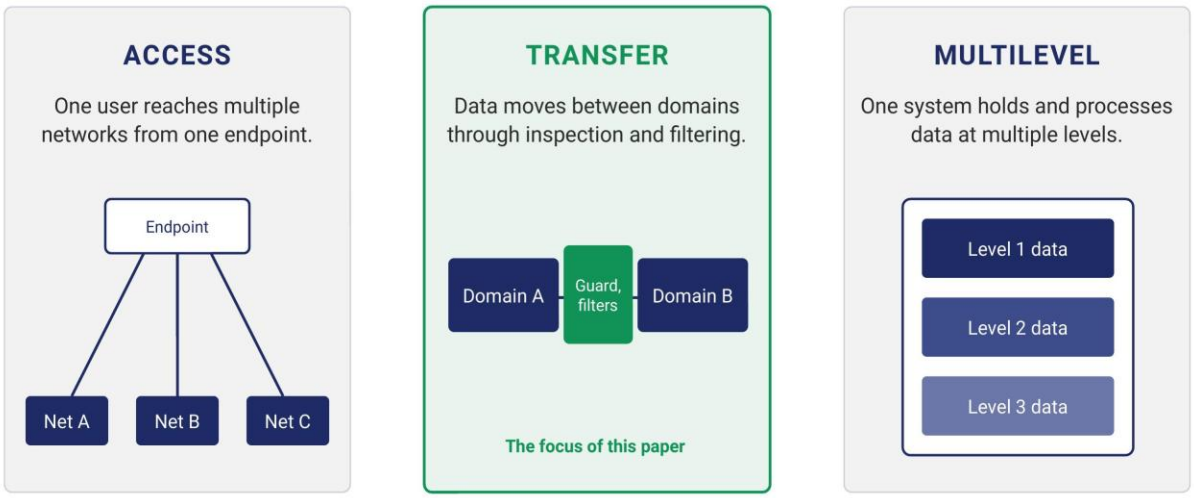

Figure 2. The three cross-domain solution types in public NCDSMO material: Access, Transfer, and Multilevel [1].

1.2 Anatomy of a transfer solution

A transfer CDS places a protocol break on each side of an inspection and filtering pipeline. Sessions terminate at the boundary. Content is validated and filtered field by field under programmable rule sets. Traffic then re-originates on the far side. There is no routable path between the domains. The one-way variant enforces direction physically: a data diode is hardware that permits transmission in one direction only. Full transfer solutions combine these elements with policy enforcement and audit.

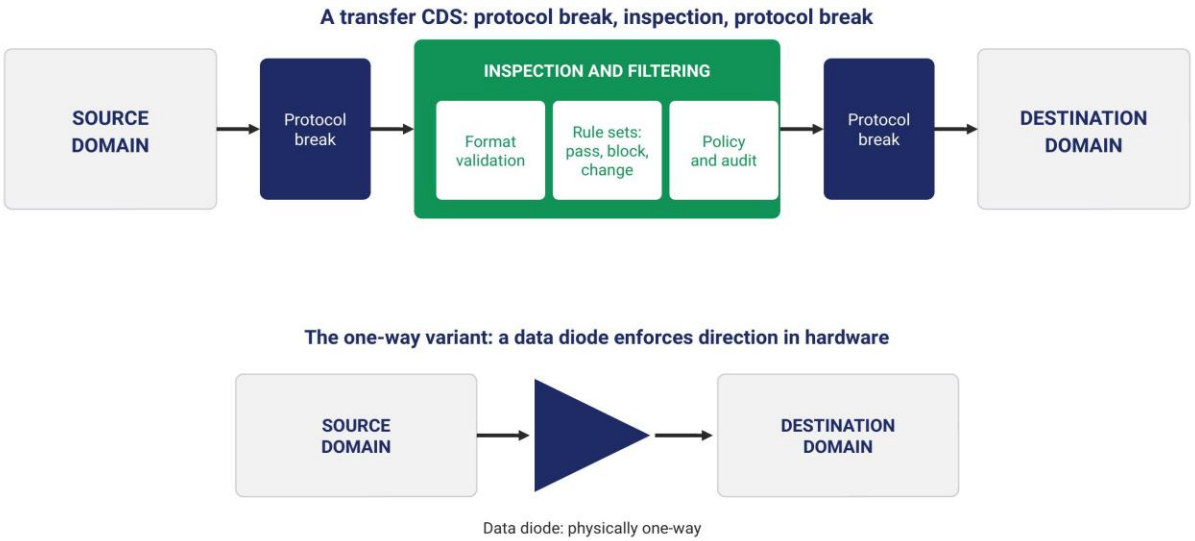

Figure 3. Anatomy of a transfer CDS (top) and the hardware-enforced one-way variant (bottom).

1.3 The accreditation ecosystem

NCDSMO publishes the security requirements for cross-domain solutions used by the U.S. Government. These requirements are known as Raise the Bar (RTB) and were first released in 2018 [1][2]. Solutions are evaluated through lab-based security assessment (LBSA). Those that meet the requirements are listed on the NCDSMO Baseline, the catalog of assessed cross-domain products [1]. Deployments into specific environments are authorized through the SABI and TSABI processes referenced in DoD cross-domain policy [3]. National Security Memorandum 8 directed agencies operating cross-domain solutions connected to national security systems to report progress toward Raise the Bar [4].

1.4 Terminology used in this paper

- **High side / low side:** the more-classified and less-classified domains on either side of a boundary.
- **Guard:** a transfer CDS that inspects and filters content.
- **Data diode:** hardware enforcing one-way transfer.
- **Rule set:** the programmable pass, block, or change logic a guard applies to each field.
- **Protocol break:** session termination and re-origination at the boundary.
- **NCDSMO Baseline:** the public catalog of assessed CDS products [1].
- **LBSA:** lab-based security assessment.
- **SABI / TSABI:** the processes for authorizing cross-domain connections at the Secret and Top Secret levels respectively [3].

2. The Gap: Movement Without Computation

Defense organizations hold large volumes of operational, intelligence, and mission data. It sits in enclaves at different classification levels, in different services, and with different coalition partners. Accredited cross-domain solutions solve the movement problem. They provide hardware-enforced transfer, filtering, and isolation between domains, from data-center guards to resource-constrained (SWaP-C constrained) devices at the edge.

What no transfer mechanism solves is the computation problem. To analyze low-side or partner-held data today, there are two choices. The first is to move the data up, which brings footprint, latency, staleness, and re-accreditation burden. The second is a manual release and disclosure process, which takes days to weeks and exposes the analyst's interest to every human in the chain. In Denied, Disrupted, Intermittent, and Limited (DDIL) environments, moving data at scale is often impossible. In coalition settings it is often prohibited. In practice, many such questions are simply not asked. No automated mechanism has existed for asking them safely.

Our approach is to move the query rather than the data. An encrypted query crosses the boundary. Only an encrypted result returns. The underlying data never moves and is never exposed. This approach automates a class of queries that are currently manual or infeasible.

3. Sovereignty: Control Without Isolation

Sovereignty pressure is reshaping allied procurement. Nations increasingly require that data remain in-jurisdiction, under national keys, on infrastructure they control. AI built on that data must respect the same constraints. Implemented purely as isolation, these requirements prevent coalition collaboration. Implemented cryptographically, they need not.

- **Data sovereignty:** data never leaves its domain and is never decrypted outside it; each nation or program holds its own keys.
- **Operational sovereignty:** the Duality platform is customer-managed software running on the customer's own cloud, on-premises, hybrid, or air-gapped infrastructure; Duality itself never accesses the data.
- **Technological sovereignty:** the cryptography is open-standard, lattice-based FHE rather than a proprietary implementation. Duality's team is a leading contributor to OpenFHE, an open-source library originally funded by the U.S. DoW. The library conforms to ISO homomorphic-encryption standardization and aligns with emerging NIST standards, and it is export-compliant [6].

For the cross-domain ecosystem, this matters commercially. Allied customers can be offered a sovereign configuration of the same accredited infrastructure. That is an increasingly explicit requirement in European and Indo-Pacific procurements.

4. How Secure Query Complements a Cross-Domain Boundary

Duality's secure query capability is enabled by FHE. Computation is performed directly on ciphertext. The low side or partner domain executes the search without ever seeing the query terms, the selectors, or the results. Only the requesting side holds the decryption key. The query is a single round trip: one encrypted request crosses the boundary, and one encrypted response returns. The cross-domain platform remains the sole transit path and the sole policy enforcement point between domains.

Some readers will recognize this pattern as query in place. Federated and data-mesh architectures already move the computation to the data instead of centralizing the data. Those architectures still expose the query and the results to the system that holds the data. That exposure is acceptable inside a single trust domain. It fails across security boundaries, where the question itself may be sensitive or classified above the data owner's level. Secure query keeps the query-in-place architecture and removes the exposure. It is query in place across trust boundaries.

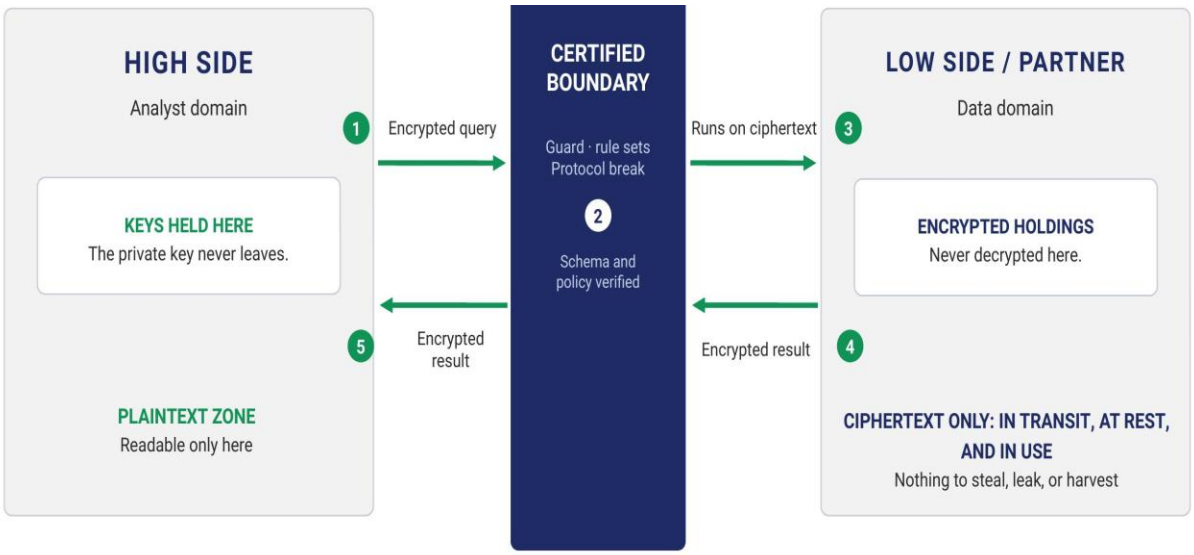

Figure 4. End-to-end flow of a Duality secure query: plaintext exists only in the analyst domain; everything crossing or executing beyond it is ciphertext.

- **No data movement:** encrypted queries cross the boundary and only fixed-format encrypted results return; no raw data is copied to the high side.
- **Full confidentiality:** the queried side never sees the query terms or the results; only the high side decrypts.
- **Bidirectional by policy, not by openness:** the return path carries only structured ciphertext responses, subject to the boundary's rule sets.
- **Post-quantum:** FHE is lattice-based and quantum-resistant, aligned with NSA CNSA 2.0 [7] and zero-trust requirements [8].

5. Accreditation: Secure Query Through a Raise the Bar Boundary

The immediate technical objection is well founded. RTB-aligned guards inspect and filter content, and an FHE payload cannot be inspected. The accreditation case therefore does not depend on payload inspection. It is built on what the boundary can verify and enforce. Ciphertext is treated as a strictly structured message type, not as opaque traffic.

- **Fixed schema:** deterministic ciphertext formats; field types, sizes, and structure are validated at the guard.
- **Programmable rule sets:** pass, block, or change decisions on every field the rule set can see, consistent with how accredited transfer solutions filter structured message formats today; there is no general-purpose channel.
- **Protocol break:** sessions terminate and re-originate at the boundary; no routable path exists across domains.
- **Bounded channel:** rate, size, and destination policy limit covert-channel capacity in both directions.

VERIFIED AND ENFORCED AT THE GUARD	HIDDEN BY DESIGN, EVEN FROM THE GUARD
• Sender identity and authorization • Message format, schema, and field sizes • Rule set verdict on every field • Rate, volume, and destination policy • Response shape: fixed-format encrypted results only	• Query terms and selectors • Result contents • Analyst intent and areas of interest

Where a program requires hardware-speed bulk analytics rather than maximum cryptographic assurance, the same architecture supports Trusted Execution Environments (TEEs) as the execution layer, with FHE reserved for the most sensitive crossings, allowing the protection mechanism to be matched to data sensitivity on a per-program basis (Section 8). Public NCDSMO statements describe the assessment path for cross-domain capabilities [1][3]. Solutions undergo lab-based security assessment against the published Raise the Bar requirements. Successful solutions are listed on the Baseline. Deployments are authorized through the SABI and TSABI processes. The natural path for the pattern described here follows that same route, on an existing accredited base, rather than as a new boundary type. Further technical detail is available to qualified parties under NDA.

6. What the Combined Capability Changes for the Mission

6.1 Worked example: querying a forward sensor archive over a commercial LEO link

ASSUMPTIONS (representative planning values; rerun with program-specific numbers)	
Forward archive	2 TB accumulated over 30 days (FMV, SIGINT metadata, imagery)
Reachback link (commercial LEO, Starlink-class)	10–25 Mbps up, 50–200 Mbps down, 25–60 ms latency
Link availability (contested)	30–50% duty cycle
Secure query payload	single-digit to tens of MB (representative)
Encrypted result payload	similar scale to the query (representative)
Query compute	seconds for representative query workloads (representative)

Option 1, move the data. Hauling the 2 TB archive to the high side consumes the constrained uplink direction. At a sustained 20 Mbps, the transfer takes just over nine days of continuous transmission. At a 30–50% duty cycle in a contested environment, it takes roughly two and a half to four weeks. The copy must then be stored, re-protected, and accredited on the high side. It is stale on arrival. The transfer is also a long-duration emission signature. If it is protected in transit by classical cryptography, it is a 2 TB harvest-now-decrypt-later liability.

Option 2, today's practical alternative. The analyst submits a request through a manual release and disclosure process. Turnaround is days to weeks. The request itself reveals the analyst's interest to every human in the chain. Most questions are never asked at all.

Option 3, move the question. The node encrypts at collection and holds its archive locally. The analyst's secure query crosses the boundary in seconds. It is encrypted under FHE and is single-digit to tens of megabytes in size. The encrypted result is of similar scale and returns in seconds to minutes, including compute. The link carries megabytes instead of terabytes. The exchange completes inside a brief transmission window compatible with emissions control. Nothing in transit reveals intent or content. The payloads are lattice-protected, so they provide no material of value for later cryptanalysis. A request that previously required days to weeks completes as a sub-minute round trip through the existing accredited boundary. On constrained links, this reduction determines whether the analysis is feasible at all.

6.2 Loss-and-capture survivability

Consider the same forward node, overrun or lost. It provides an adversary with no plaintext holdings, no readable query history, and no record of collection interest. Encryption at collection, combined with secure query, substantially reduces the consequence of platform loss. For systems operating forward, this is a survivability property as well as an analytics capability.

6.3 Insider threat and cryptographic need-to-know

Query patterns are themselves sensitive. Records of who searched for what have been exploited in insider-driven compromises. With secure query, the analyst's interest is hidden even from the administrators of the queried infrastructure. Need-to-know is enforced cryptographically rather than procedurally. The platform's audit trail (Section 9) completes the picture. Query content is hidden from the data side, while authorization for every query remains verifiable. The result is compartmentation with accountability.

6.4 Harvest now, decrypt later

Data crossing boundaries today is being collected today, for decryption by future quantum capability. Most of what crosses a guard has a sensitivity horizon of ten years or more. For that data, post-quantum protection is a present requirement rather than a future one. National Security Memorandum 10 reflects this concern [9]. FHE's lattice-based construction is aligned with NSA CNSA 2.0 [7]. It protects these flows against such collection from initial deployment.

7. Operational Patterns

7.1 Cross-domain secure query

A high-side analyst issues a query that fans out, encrypted, to multiple data owners across the boundary. The owners may be separate enclaves, separate agencies, or separate nations. Each data owner executes the query on ciphertext and returns encrypted results. Results are aggregated and decrypted only on the high side.

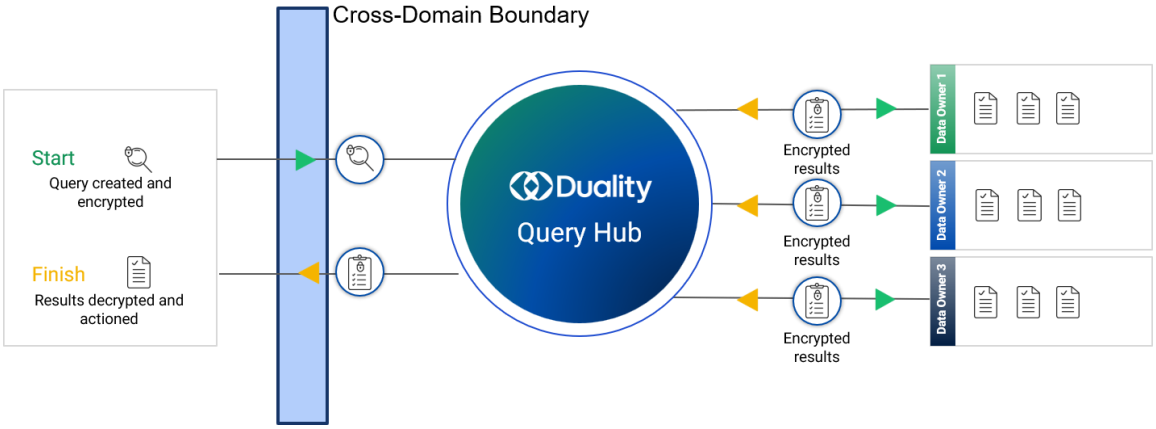

Figure 5. Cross-domain secure query flow across multiple data owners.

7.2 Zero-footprint investigation at the tactical edge

Edge collection platforms encrypt at the point of collection. They range from sensors to mobile handsets, and they store to whatever transport is available, including commercial cloud. Analysts pull what the mission needs through encrypted queries. Streaming searches run without exposing the target

of interest. Semantic and multi-modal queries run across text, audio, and video. Entity resolution runs without revealing the subjects of interest.

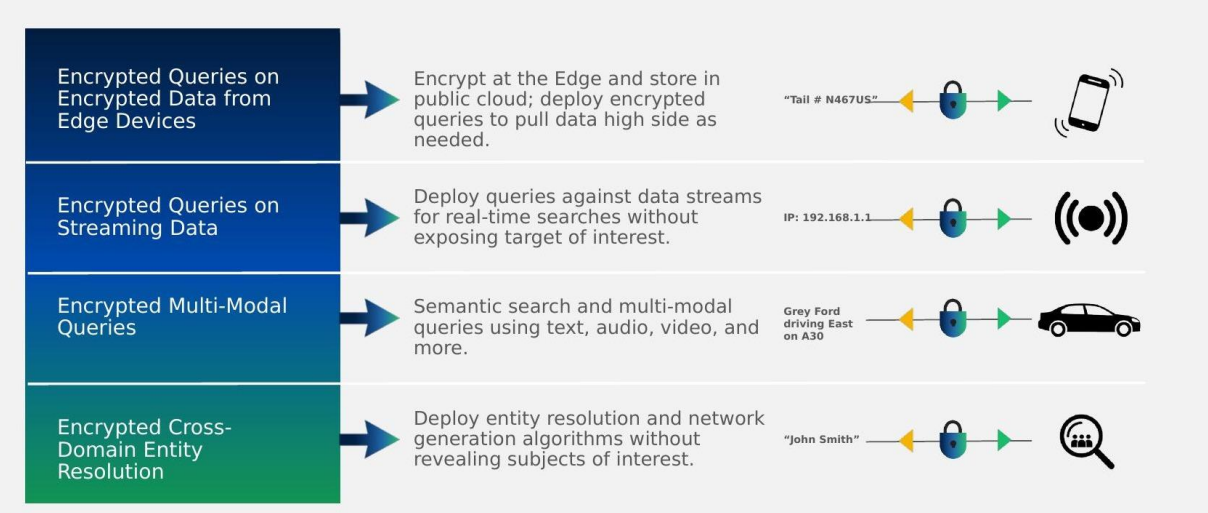

Figure 6. Variations of zero-footprint investigation over encrypted holdings.

7.3 Cross-domain biometric and multi-modal search

Consider an analyst who cannot reveal that they know what a target looks like. With secure query, they search a partner-held biometric database using an encrypted probe. The data owner computes similarity entirely on ciphertext and returns encrypted candidates. Only the analyst decrypts. The same pattern applies to any high-value selector: imagery of a named area of interest, supply-chain and vulnerability lookups, or watchlist checks between partners who cannot pool raw data.

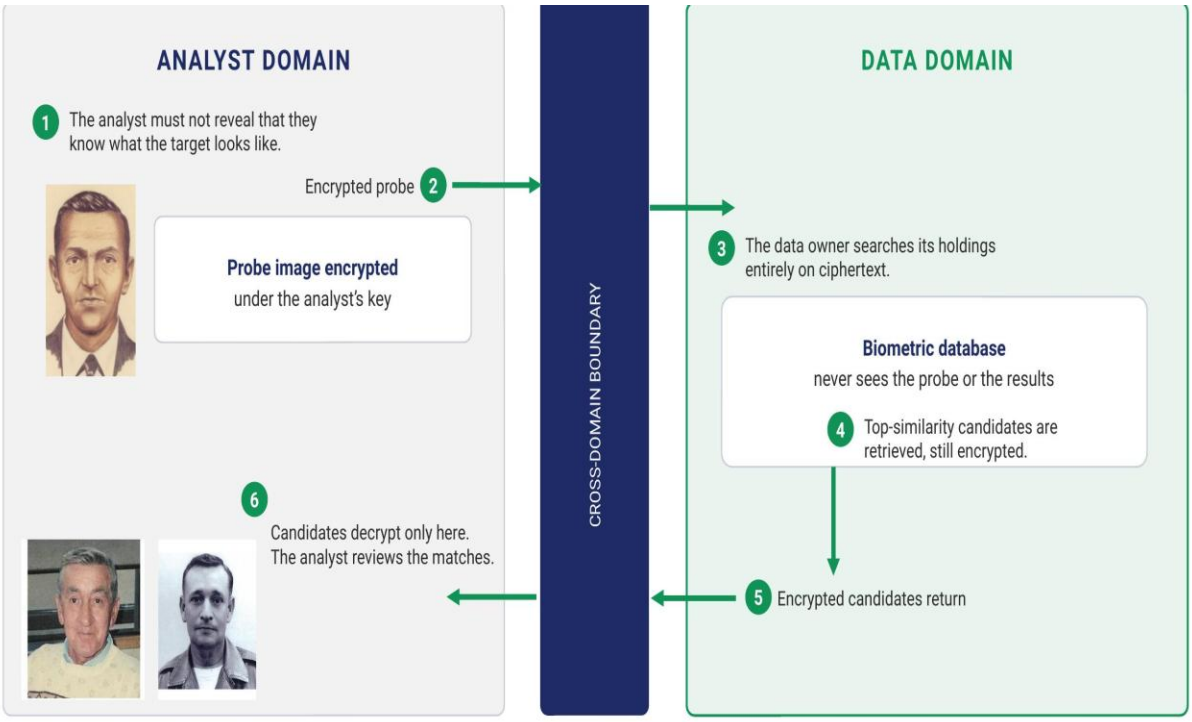

Figure 7. Cross-domain biometric search: encrypted probe, encrypted match, high-side decryption.

7.4 Coalition and federated analytics

The roles map naturally onto a coalition. Each nation is a data owner with its own keys. The analyst nation is the analyzing party. A control plane governs who may compute what. The accredited CDS is the only transit path. On that foundation, the same architecture supports federated analytics and AI. Datasets that cannot be combined can still be analyzed together: they may sit on different networks, in different sovereignties, or collation may raise the aggregate classification. Models can be trained, tuned, and tested against data that never leaves its owner. This supports coalition interoperability without a shared data lake.

8. Beyond Query: The PET Portfolio on a Cross-Domain Foundation

Secure query is the initial integration point, not the extent of the portfolio. Duality operationalizes the full family of privacy-enhancing technologies: FHE, Trusted Execution Environments, federated learning, multi-party computation, and differential privacy. They run individually and in combination, under one policy and audit plane. The division of labor is simple. A guard controls what crosses. A TEE controls what happens on either side. FHE controls what is exposed in between. The patterns below layer directly on the same accredited foundation.

- **Confidential AI on partner infrastructure (shipping):** TEE clusters with GPU acceleration run large-model inference and training with the model, prompts, and outputs protected throughout; through Red Hat OpenShift confidential containers they run on-premises, in air-gapped and sovereign environments, with attestation of the actual workload and no public-cloud dependency.
- **Hybrid FHE and TEE (shipping):** FHE runs inside the enclave for the most sensitive retrievals, combining cryptographic protection for the most sensitive operations with hardware-speed execution elsewhere; this is the configuration referenced in Section 5.
- **Encrypted semantic search and RAG (shipping):** privacy-preserving search extends beyond structured records to documents, text, and knowledge bases, powering retrieval-augmented generation where prompts, retrieved content, and outputs never leave the trusted environment. For defense: LLM-assisted analysis over sensitive holdings without exposing either the data or the question.
- **Federated learning with protected updates (shipping):** models train locally at each site (each nation, each enclave); intermediate updates are aggregated inside a TEE or under FHE, closing the leakage path standard federated learning leaves open. A diode or guard is the natural transit point for those updates.
- **Model IP protection and coalition model exchange (emerging):** a model owner deploys into a data owner's environment without revealing weights, and the data owner runs the model without visibility into it. This is the converse of the data-protection case: the CDS physically contains edge AI, central command queries it cryptographically, and the model owner's intellectual property is not exposed.

- **Cross-domain agentic AI (emerging):** MCP-mediated agents that can ask about data on other domains without any raw-data channel existing: governed, auditable, rule-set-constrained agent queries through the boundary.

Items are labeled shipping or emerging deliberately: the operational capabilities carry the near-term program value, and the emerging patterns indicate areas suitable for joint reference-architecture development.

9. Governance and Auditability

Encryption that defeats oversight would be disqualifying in this domain. The Duality platform is therefore governed by a control plane, the Collaboration Manager. It defines who is allowed to compute what. It enforces that policy during the computation itself. It orchestrates the workflow across participants, and it produces a complete audit trail. A collaboration runs in five steps. Policy is set. Data stays in place with its owner. The approved computation runs. Only the agreed result is released. Every step is logged and cryptographically enforceable.

Two properties matter for defense programs. First, policy is enforced at the level of the computation, cryptographically rather than contractually. Content is hidden; authorization is provable. Second, Duality is delivered as customer-managed software. Duality itself never accesses the underlying data, keys, or models. Vendor access is precluded by the architecture, not by contractual agreement.

10. Alignment with Data-Centric Security

The direction of travel, set out in the DoD Zero Trust Strategy [8], is data-centric security: tagged and labeled data objects, attribute-based access control, and enterprise ICAM as the decision fabric. SECD is architecturally aligned with that stack. It completes the stack for data in use. The guard enforces label and attribute policy on the envelope. FHE protects the payload's content and the query's intent. The audit plane records attribute-checked decisions. Access control governs who may touch a data object. Secure computation governs what can be learned from it. Integration with tagged data formats and program ICAM attribute sources is addressed as part of a joint reference architecture.

11. Integration in Practice

Secure query is delivered as software and is designed to be integrated by others: by CDS vendors into product roadmaps, by integrators into programs, and by government engineering teams into existing mission systems. This section describes what an integration consists of.

11.1 Where the components sit

The architecture places a query orchestration component on the analyst (high) side and a compute component alongside the data on the low or partner side. Neither component sits inside the boundary, replaces any element of it, or requires modification to it. The boundary continues to carry traffic exactly as it does today; the only change visible to it is a new, strictly structured message type whose schema its rule sets validate. Keys are generated and held on the analyst side under the operator's existing key-management practice; the compute side holds only public evaluation keys.

11.2 Interfaces

Integration surfaces are conventional. Backend interfaces are exposed through APIs and SDKs across C++, Python, Rust, and other common languages, so secure query can be embedded in existing analyst tools, data platforms, and workflow engines rather than introduced as a separate destination. For agentic and LLM-based workflows, Model Context Protocol (MCP) interfaces allow AI agents to issue governed queries against sensitive data without any raw-data channel existing. For operators, a drag-and-drop analytic interface requires minimal training and no change to operational flows.

11.3 Deployment models

The platform is customer-managed software. It runs on cloud, on-premises, hybrid, air-gapped, and disconnected infrastructure, and is containerized for modern orchestration environments. No custom hardware is required on either side of the boundary, and no vendor-operated service is in the path: Duality never touches customer data, keys, or models. This matters for cross-domain programs specifically, because it means the addition of secure computation introduces no new external dependency into an accredited environment.

11.4 Working with existing rule sets

The integration artifact a cross-domain engineering team actually consumes is a message specification: deterministic ciphertext formats with fixed field types and sizes, published so that guard rule sets can validate structure, enforce size and rate policy, and log verdicts. Rule-set development, tuning, and accreditation support follow the same engineering process the community already applies to any new structured data type crossing a boundary.

12. Working with the Cross-Domain Ecosystem

Duality is a complement to the cross-domain ecosystem, not a competitor within it. Duality builds no guards, diodes, or filters, seeks no boundary approvals of its own, does not act as a systems integrator or prime, and never holds customer keys, data, or models. The intent is that secure computation becomes a capability of the ecosystem, delivered through the vendors, integrators, and programs that already own the boundary.

12.1 For CDS vendors

For vendors of accredited Access, Transfer, and Multilevel solutions, secure query is a candidate capability layer for existing product lines: a new class of structured traffic that existing filtering architectures can validate, and a computation capability that extends what an accredited transfer path can be used for without altering what it is. The natural collaboration artifacts are joint message-format specifications, reference configurations for specific product families, and co-developed rule-set templates.

12.2 For primes and systems integrators

For integrators, the delivery model is deliberately service-heavy on the integrator side. Duality supplies software and cryptographic engineering support; mission integration, rule-set engineering, accreditation support, deployment into program environments, training, and lifecycle sustainment are performed by the integrator. Program adoption therefore expands the integrator's engineering and sustainment work in addition to software licensing. A practical first engagement is a scoped joint integration: secure query on an accredited transfer boundary against one agreed mission thread, assessed jointly, with results feeding a shared reference architecture.

12.3 For program offices and accreditors

For programs, the relevant properties are what the pattern does not ask for: no new boundary type, no modification to accredited components, no general-purpose channel, and no vendor in the data path. What it does ask for is the normal engineering work of admitting a new structured message type: schema review, rule-set development, and assessment on the existing base, consistent with the publicly described Raise the Bar assessment process [1]. Independent evaluation of the combined pattern is welcomed.

About Duality Technologies

Duality develops software for privacy-enhanced data and AI collaboration. Founded and led by cryptographers and data scientists, Duality operationalizes privacy-enhancing technologies, including Fully Homomorphic Encryption, trusted execution environments, and federated learning, to enable analysis and model learning while preserving privacy, security, compliance, and intellectual property. Duality's FHE lineage runs through more than a decade of DARPA-funded research, including the DPRIVE hardware-acceleration program [5], and its team is a leading contributor to the open-source OpenFHE library [6]. PETs are the subject of a growing body of public guidance, including the UN Guide on Privacy-Enhancing Technologies [10].

Advisors include Admiral Mike Rogers (fmr. NSA Director), General Sir Chris Deverell (fmr. Commander, UK Joint Forces Command), and Sir Jeremy Fleming (fmr. Director, GCHQ).

Ten Questions We Expect From the Cross-Domain Community

1. How does uninspectable ciphertext pass a Raise the Bar guard?

The guard never inspects payload semantics for any encrypted format; it verifies structure. Fixed, deterministic ciphertext schemas let the guard validate format, field types, sizes, sender authorization, and destination policy, with a full protocol break at the boundary.

2. Isn't the return path an exfiltration channel?

Only fixed-format encrypted results may return, subject to the same rule sets, with rate, size, and destination caps. There is no general-purpose channel in either direction.

3. What about covert channels in ciphertext size or timing?

Formats are deterministic and sizes are fixed per query class; rate and volume policy bound residual channel capacity. Assessment artifacts are available under NDA.

4. What happens if high-side keys are compromised?

Private keys never cross the boundary, so a compromise exposes only results decrypted after that point, never the partner's holdings. Keys rotate under normal enterprise key-management practice.

5. How does it perform over degraded or DDIL links?

A query is a single round trip of megabyte-scale payloads. WAN and satellite latency add transport time but not exposure; see the worked example in Section 6.

6. Is FHE actually fast enough?

Field-wide FHE performance has improved by orders of magnitude over recent years, driven by algorithmic advances, compilers, batching, and DARPA program investment [5]. Representative benchmark data is available to qualified parties under NDA.

7. How are keys managed across domains and coalition partners?

Each domain or nation holds its own private keys, which never leave; only public evaluation keys are distributed. There is no shared secret across the coalition.

8. Does this replace our guards, filters, or diodes?

No. The certified boundary remains the sole transit and enforcement point. Duality is a computation layer that rides on it; we build no boundary hardware.

9. What is the accreditation path?

The path described in public NCDSMO statements: lab-based security assessment against the published Raise the Bar requirements on an existing accredited base, with deployment authorized through SABI/TSABI, not a new boundary type [1][3].

10. What about quantum computers?

FHE is lattice-based and aligned with NSA CNSA 2.0. Flows are protected against harvest-now-decrypt-later collection from initial deployment.

References

[1] National Cross Domain Strategy and Management Office (NCDSMO), "Fundamentals of Cross Domain Solutions," approved for public release (DOPSR case #23-S-1103), NDIA Systems and Mission Engineering Conference, 2024. https://ndia.dtic.mil/wp-content/uploads/2024/systems/O-D_De_Silva.pdf

[2] National Security Agency, National Cross Domain Strategy and Management Office homepage. https://www.nsa.gov/Cybersecurity/Partnership/National-Cross-Domain-Strategy-Management-Office/

[3] U.S. Department of Defense, DoD Instruction 8540.01, "Cross Domain (CD) Policy." https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/854001p.pdf

[4] The White House, National Security Memorandum 8, "Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems," January 19, 2022.

[5] Defense Advanced Research Projects Agency, Data Protection in Virtual Environments (DPRIVE) program. https://www.darpa.mil/program/data-protection-in-virtual-environments

[6] OpenFHE open-source fully homomorphic encryption library. https://www.openfhe.org

[7] National Security Agency, "Announcing the Commercial National Security Algorithm Suite 2.0," Cybersecurity Advisory, September 2022. https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

[8] U.S. Department of Defense, "DoD Zero Trust Strategy," November 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

[9] The White House, National Security Memorandum 10, "Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," May 4, 2022.

[10] United Nations Committee of Experts on Big Data and Data Science for Official Statistics, "UN Guide on Privacy-Enhancing Technologies for Official Statistics," 2023. https://unstats.un.org/bigdata/task-teams/privacy/guide/