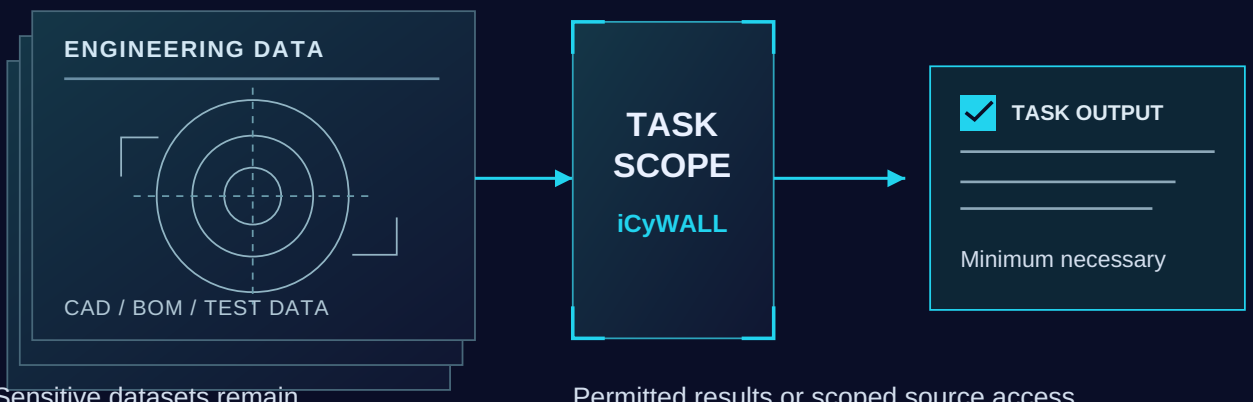
Collaborate without losing control.

Protect sensitive industrial data. Give subcontractors only the information or result their approved task requires.

INDUSTRIAL & AEROSPACE / SECURE SUBCONTRACTOR COLLABORATION

CLIENT-HELD ASSETS

APPROVED COLLABORATION



Sensitive datasets remain under client control.

Permitted results or scoped source access. Matched to the approved task.

PILOT TARGETS — TO BE VALIDATED · SEE SCOPE ON PAGE 05

70%
Lower data exposure

100%
Vendor-access traceability

~40%
Faster supplier onboarding

THE BUSINESS CHALLENGE

Access is not evidence of use.

Industrial and aerospace companies rely on multi-partner supply chains to design, manufacture, maintain and certify complex products. That collaboration requires subcontractors to work with sensitive engineering and production assets.

The problem begins when collaboration turns into **copy and transfer**. Once sensitive information leaves the controlled environment, visibility and enforceable usage control deteriorate.

A login record may confirm that a vendor entered a system. It does not, by itself, establish what happened to the data after access was granted.

Every additional supplier expands the identities, sessions, devices, datasets and contractual boundaries that must be governed.

Sensitive assets

CAD files · BOMs · Specifications
Test results · Production data

THE SUPPLIER BLIND SPOT

Who logged in is only the first question.

- ? Was the file copied?
- ? Reused beyond the project?
- ? Forwarded to another subcontractor?
- ? Retained after the engagement?

From access control to usage control

The traditional workflow

Approve a user, authenticate a session, grant a permission and log a connection. These controls remain necessary, but do not preserve control over a dataset already copied outside the environment.

The governed alternative

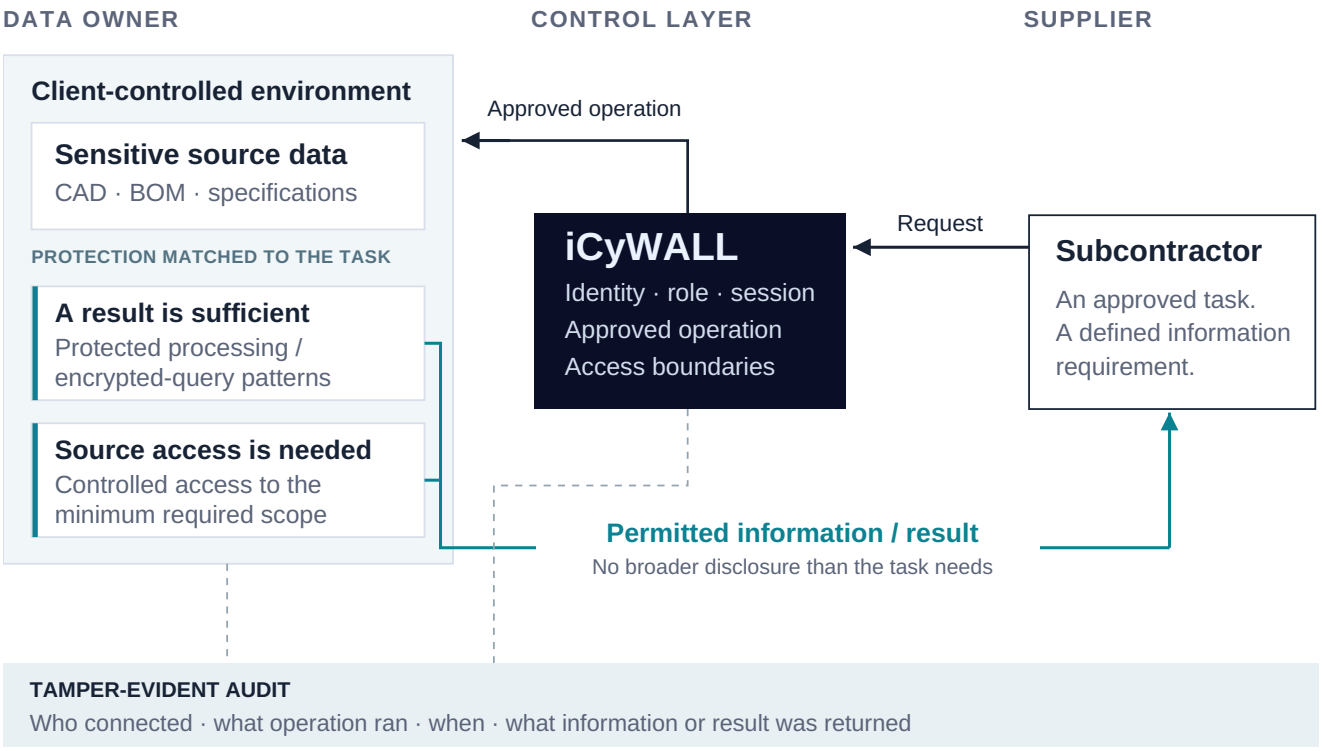
Define the task, limit source access or return a permitted result, and retain evidence of the material interaction. Collaboration remains useful without making unrestricted external sharing the default.

Give suppliers what the task needs— not unrestricted data access.

THE AIDATACY APPROACH

Share the result. Control the interaction.

Combine protected data processing, iCyWALL-controlled supplier access and tamper-evident evidence. Match the level of exposure to the approved task—not to a broad repository permission.[4]



Conceptual workflow based on the use-case source. The two task paths are alternatives: protected processing when a result is sufficient; minimum-scope source access when the work requires it.

When a result is enough

For an approved query, matching operation, validation, scoring or other constrained computation, protected-processing and encrypted-query patterns can return the result without exposing the full underlying dataset.

When source information is needed

Restrict access to the minimum information necessary for the task. Record who connected, the approved operation, when it occurred, and the information or result returned.

The objective is not to eliminate all sharing. It is to eliminate unnecessary exposure.

IMPLEMENTATION

Make controlled collaboration repeatable.

Six steps from supplier exposure to controlled collaboration. Establish the task, protection boundary and evidence requirements before extending the model.

01 **Diagnose**

Map subcontractors, vendor access paths, sensitive datasets, and current data-sharing flows.

OUTPUT

Vendor access and data-flow assessment

02 **Define**

Identify critical exposure points, supplier roles, allowed operations, and audit requirements.

OUTPUT

Collaboration control model

03 **Deploy**

Apply the appropriate protection model to each collaboration flow, based on whether the supplier needs source-data access or only a derived result.

OUTPUT

Protected collaboration environment

04 **Pilot**

Validate controlled supplier sessions, allowed operations, data-exposure boundaries, and end-to-end traceability with selected subcontractors.

OUTPUT

Validated supplier-access pilot

05 **Operationalize**

Activate tamper-evident logging, monitoring, anomaly detection, and compliance reporting.

OUTPUT

Auditable supplier operations

06 **Production**

Continuously score risk and scale the model across the subcontractor and supply-chain ecosystem.

OUTPUT

Controlled multi-partner collaboration

Deployment roadmap

PHASE 1	PHASE 2	PHASE 3	PHASE 4	PHASE 5
Vendor mapping + risk scoring	Deploy iCyWALL (access-control layer)	Integrate encrypted query engine	Enable audit + monitoring	Scale to full supply chain

BUSINESS IMPACT

Less exposure. Stronger supplier evidence.

Reduce unnecessary data exposure, improve supplier activity traceability and reuse a governed access pattern instead of rebuilding a bespoke process for every engagement.

PILOT TARGETS — TO BE VALIDATED

70%

Lower data exposure

Target reduction through less full-data transfer and protected result sharing. Source access remains limited to the minimum required scope when a task needs it.

100%

Vendor-access traceability

Target coverage at the **defined controlled-session and interaction layer**. The scope is not visibility into every activity outside the controlled environment.

~40%

Faster supplier onboarding

Target improvement through standardized protected access, session controls and audit requirements—not a reported production result.

Targets are retained from the linked UC 04 source and require pilot validation against agreed baselines. The workbook outline uses "↓ 70% data exposure", "100% vendor access traceability", and "Faster onboarding supplier (~ -40%)". The linked source describes onboarding as approximately 40% faster; these formulations have not been recalculated as equivalent measures.

NIS2-aligned control evidence

NIS2 Article 21 addresses cybersecurity risk-management measures including supply-chain security, access control and cryptography. Relevant EU implementing requirements and ENISA guidance also address supplier policies, contractual requirements, incident notification and audit rights.[1–3]

Supplier roles & permitted operations

A defined collaboration control model makes supplier roles, allowed operations and exposure boundaries explicit.

Access control & protected processing

Task-scoped sessions and the appropriate protection model limit unnecessary exposure of sensitive information.

Audit evidence & incident review

Tamper-evident interaction records and monitoring support review, reporting and supplier-activity traceability.

Reference framework: Directive (EU) 2022/2555 and Commission Implementing Regulation (EU) 2024/2690, with ENISA implementation guidance. Control alignment is not a claim of certification or automatic compliance.

NEXT STEPS

Start with the next supplier engagement.

FROM EXPOSURE TO A CONTROLLED WORKFLOW

Assess Your Supplier Collaboration Exposure

Start with a high-value supplier workflow. Identify where sensitive information leaves the controlled environment and which tasks genuinely need source-data access.

- → Map vendors, access paths, sensitive datasets and current sharing flows.
- → Define allowed operations and the minimum information required for each task.
- → Pilot controlled sessions, interaction evidence and target improvements against agreed baselines.

contact@aidatacy.com

aidatacy.com ↗

References & sources

01 EUR-Lex - Directive (EU) 2022/2555 (NIS2), Article 21 cybersecurity risk-management measures
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02022L2555-20221227

02 EUR-Lex - Commission Implementing Regulation (EU) 2024/2690, supply-chain security requirements
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R2690

03 ENISA - Supporting NIS2 implementation through actionable guidance
https://www.enisa.europa.eu/news/supporting-nis2-implementation-through-actionable-guidance

04 AIDATACY - secure data collaboration and infrastructure capabilities
https://www.aidatacy.com/

Source basis: “USE Case AML.xlsx”, UC 04 EN narrative, original use-case outline and linked UC 04 document. Source descriptions and URLs are preserved above.