



Who Gets In, to What, and for How Long: A Unified Approach to OT Sovereignty

Security for an industrial project does not end at the control panel. Engineers need access to configure, commission, troubleshoot, and support the systems they deliver. The customer needs confidence that this access serves the job without becoming an uncontrolled route into the plant. That is where OT sovereignty becomes practical: deciding who may do what, on which assets, and when that permission ends.

For a plant leader, this comes down to delivering useful work without losing authority over the environment where that work happens. An integrator should be able to commission a machine center, diagnose a fault, and support the installation without treating the surrounding plant as part of the assignment. The customer should be able to see the boundary, approve it, and withdraw access without negotiating the return of control.

Kasm Workspaces and Xiid Terniion bring that objective into the engineering workflow. Kasm controls the working environment; Xiid controls what it reaches. Together, they give customers a practical way to bring expertise to the job while keeping the tools, communication paths, and continuing support arrangement within an agreed scope. Our approach starts with the work the customer needs done and carries that boundary through commissioning, handover, and maintenance.

Two boundaries, one engineering job

Authorizing an engineer to work on a packaging machine should scope access to that specific assignment, and the working environment and its connectivity should reflect the same decision.

Kasm supports container-based workspaces and server-based workspaces using RDP, VNC, and SSH. This gives the project team options for presenting the desktop or application the engineer needs. Select the environment around the actual tool, including its operating system, licensing, and project-file requirements. Where the task calls for an existing engineering workstation, evaluate that workflow rather than assuming every application belongs in a container.

Terniion's data plane uses agents at either end to establish outbound-only tunnels between specific processes. Commander manages connection policy, and the Connector joins the outbound communication halves without decrypting their traffic. Configure those relationships around the approved working process and maintenance destination, so connectivity stays scoped to the task and never expands into general network reach.

The value is a clear division of control: provide the right place to work, then define the paths that work requires. Application permissions and plant change procedures govern what the engineer may do within that scope. The customer gains access to expertise without handing the specialist an open-ended assignment.

The value is a clear division of control: provide the right place to work, then define the paths that work requires.

Begin with the job at hand

Start with a real engineering job: the machine center, the required tools, the people involved, and the systems they must contact. A commissioning engineer may need an HMI and an engineering workstation. A controls specialist may require a programming connection. A support technician may need diagnostic visibility. Shape access around those tasks, even when they concern the same equipment.

Before factory acceptance testing or site commissioning, prepare the working environment and its intended communication paths. Agree where project files will remain, how approved revisions enter the environment, and who authorizes changes in access. This makes safeguarding the work part of project delivery from the beginning, so it never becomes a separate exercise tacked onto handover.

As commissioning reveals dependencies, add them one at a time: give each change an owner and a purpose, then decide whether it belongs in the ongoing support arrangement. Operations retains authority over equipment state, maintenance windows, and approval to change a running process.

At handover, leave the customer with the approved project revision, documented access relationships, infrastructure ownership, and a usable support procedure. Narrow commissioning permissions to the support task or withdraw them. Continuing service becomes a deliberate commercial and operational choice the customer controls.

Make closure demonstrable: the agreed withdrawal procedure should end the active session and prevent a fresh connection through the withdrawn route. Coordinate the required workspace, application, and connectivity actions and verify the result. The customer keeps the delivered capability and decides when outside expertise returns.



Own the dependencies as well as the data

Customer control should extend to the infrastructure that makes the work possible.

Terniion's Connector/broker can be customer-hosted today. Customers can operate the connection infrastructure under their own authority, alongside the working environment and project data, with explicit administration and recovery responsibilities.

Plan ownership beyond the servers themselves.

Identity, name resolution, time, application licensing, backups, and recovery all belong in the deployment design. Giving those services an explicit home helps the customer retain internal maintenance capability when an integrator changes or an outside service is unavailable.

Terniion supports internal operation in disconnected environments, including air-gapped deployments.

For an all-internal disconnected mode, the required communication components and supporting services must be available inside the boundary. Internal users can work across that infrastructure without an outside maintenance connection.

Outside support is a separate, deliberate operating mode.

It requires an approved transport path across the boundary and the necessary components reachable over that path. A physically disconnected site cannot receive an outside remote session, and an outbound-established tunnel is still connected. The customer decides when to enable that path and when to remove it while preserving the internal capability it intends to keep.

Kasm provides an offline-installation licensing procedure.

Plan connected license activation and transfer, along with renewal needs, separately from everyday internal operation. This keeps licensing preparation in the deployment plan without making it the center of the maintenance workflow.

Keep project files, application data, workspace storage, and backups in customer-governed locations.

Where session recordings are required, Kasm supports a custom S3-compatible storage endpoint, with Enterprise licensing required for recording. Select storage and retention to match the customer's ownership requirements. Keeping working files in the controlled environment can reduce the need to distribute copies to personal endpoints; govern permitted transfers and remote screen access as part of the same design.

Fit the access boundary to the brownfield plant

Build around the equipment and engineering tools the customer already uses. A machine center may sit behind its own switch, control subnet, or OEM boundary. Begin at the maintenance destination, identify where Terniion's STLink can run, and choose the smallest supportable arrangement for the required workflow.

Where a legacy asset cannot host an agent, evaluate an adjacent supported host as the maintenance destination. Configure that host's last-hop reach with the plant's network and host controls so it serves the approved assets. The tunnel boundary and the host's local reach should express the same task scope.

A representative workflow trial establishes the fit: the application, its ports and discovery behavior, required drivers, and licensing dependencies. Preserve existing production-control paths while evaluating the maintenance path. This approach focuses investment on useful access to existing assets, with a defined boundary that can be repeated where the next workflow supports it.

Expertise reaches the problem while the plant retains the decisions that govern production.

ILLUSTRATIVE MAINTENANCE SCENARIO

Support for one machine center

The following scenario illustrates the approach; it is not a report of customer results.



ILLUSTRATIVE MAINTENANCE SCENARIO

A packaging machine develops an intermittent fault after handover. The plant needs the integrator's controls specialist, but only for that machine center. Operations approves diagnostic work while a local engineer remains responsible for the equipment's operating state.

The specialist receives the designated Kasm workspace and approved tools. Terniion is configured to permit the required communication to the selected maintenance destination, with neighboring machine centers outside the authorized scope. The local team confirms the machine identity, project revision, and permitted activity before work begins.

The specialist investigates using that environment. If diagnosis calls for a program change, operations approves the change and any additional permissions before it proceeds. The team then preserves the resulting project revision and records what operations are accepted. Expertise reaches the problem while the plant retains the decisions that govern production.

With Enterprise licensing and recording configured, Kasm can provide a visual record of the supported workspace session for review. Keep that record alongside the engineering change documentation and project artifacts in the agreed customer-controlled locations.

At completion, the administrator ends support access and verifies that the specialist cannot reopen the withdrawn path. The plant retains the work and its supporting records. If the fault recurs, it can authorize another session without restoring the wider commissioning arrangement. Support stays available whenever the customer chooses to authorize it, session by session.

Expertise reaches the problem while the plant retains the decisions that govern production.

Prove the boundary in practice

Bring us one machine center, one engineering workflow, and the outcome your team needs. We will work with you to define a bounded Kasm and Xiid proof of value around useful work, controlled reach, and customer ownership. Use a representative non-production environment where appropriate and agree on the operating mode before the evaluation begins.

Demonstrate the task with the actual tools and dependencies, at acceptable responsiveness under representative conditions. Then verify the boundary: the required destinations are reachable and the agreed out-of-scope destinations are denied. Demonstrate withdrawal against both an active session and a fresh reconnection attempt, using the administrative sequence defined for the deployment.

For all-internal disconnected operation, show that required internal work continues without outside connectivity. For selectively connected maintenance, show how outside access is enabled and removed while retaining the internal maintenance capability the plant expects. These demonstrations establish the operating model the customer is buying.

Follow the work through to ownership. Confirm that project artifacts reach their agreed locations and that authorized reviewers can retrieve any required recordings. Finish with a concise acceptance package showing the task completed, paths permitted and denied, dependencies identified, artifacts retained, and withdrawal outcome.

That package gives the customer a concrete basis for adoption and the integrator a repeatable delivery model. Expand to the next machine center on the strength of its workflow and requirements, carrying forward what the first evaluation established.

Plant leaders
should not have to
choose between
useful engineering
support and
meaningful control.

Leave the plant in control

Plant leaders should not have to choose between useful engineering support and meaningful control. Integrators should be able to show that safeguarding the work is part of delivering it.

Kasm provides the controlled working environment. Xiid Terniion constrains the communication paths. Applied to the customer's engineering task, they support a practical outcome: expertise can reach the work, the plant retains authority over the scope, and handover leaves a clear support arrangement under customer control.

Start with the job that matters, prove the access boundary, and leave the customer with the capability to operate, maintain, and choose who supports the installation next. Safeguard the work. Keep control of the plant.

Bring us one machine center.

Start your Kasm and Xiid proof of value.

xiid.com/contact-us