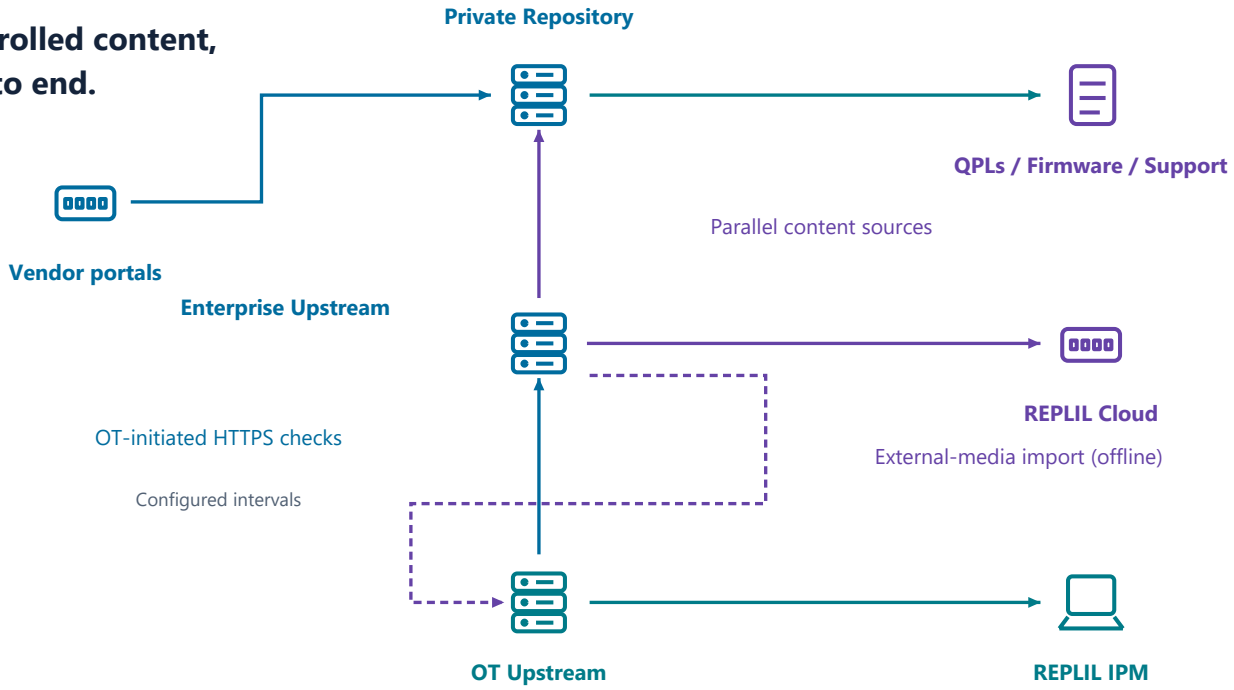
One source. Facility-wide reach.

Automate vendor-content acquisition. Bring qualified patch lists, firmware and supporting information into one controlled repository.

ARCHITECTURE / WORKFLOW

Controlled content, end to end.



A connected content workflow, from vendor acquisition to local OT availability.

CONTROLLED CONTENT. PRACTICAL OPERATIONS.

01 Multi-vendor acquisition

Connect to supported vendor portals using approved account entitlements.

02 Scheduled synchronization

Automate supported content requests and acquisition workflows.

03 Integrity and metadata

Retain metadata, checksums and hashes before controlled distribution.

04 Vendor authentication

Use supported portal authentication and keep acquisition activity auditable.

The capabilities behind the workflow.

REPLIL Private Repository - detailed product features

Multivendor portal acquisition

Acquire content from supported vendor portals using approved credentials and available vendor APIs or acquisition workflows.

Scheduled content synchronization

Automate scheduled synchronization and vendor-content requests to keep the central repository current.

QPL, firmware, and support content

Organize qualified patch lists, firmware, special patches, and other important vendor data in a controlled central catalog.

Metadata and integrity validation

Validate acquired content with metadata, checksums, and hashes before controlled distribution.

Facility-wide content availability

Make selected vendor content available centrally to Enterprise Upstream. OT Upstream checks Enterprise Upstream at configured intervals for available qualified patch lists and firmware files; Enterprise Upstream does not initiate access into OT.

Vendor authentication and audit

Use vendor-specific authentication, including MFA where supported, approved account entitlements, and an audit trail. Portal access and automation availability vary by vendor and account.

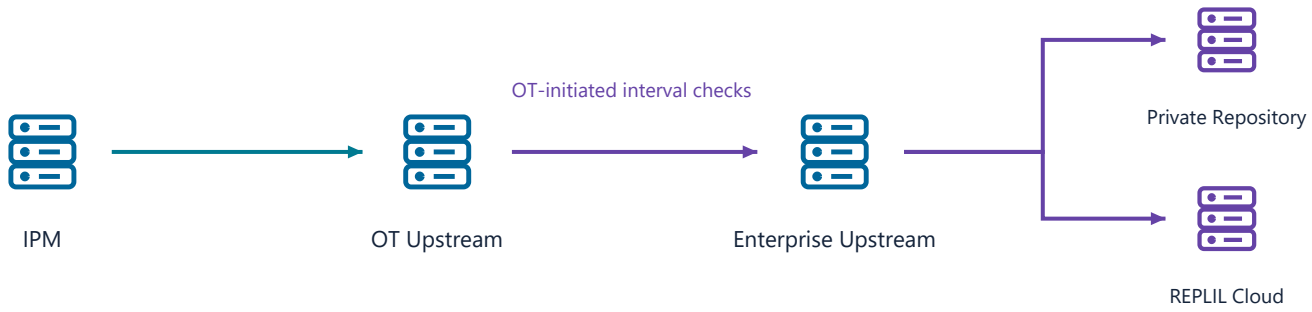
Connected and disconnected OT workflows

Support approved data-diode communication paths where deployed. Use HTTPS for OT-initiated availability checks, or prepare controlled external-media imports for disconnected OT Upstream environments.

Content capacity for the facility

Plan repository retention for multiple vendors, versions and languages. Size local Linux repositories separately for each Linux vendor type.

Make the workflow fit the facility.



HTTPS when connected; manual external-media import when disconnected.

Multi-vendor acquisition

Gather qualified patch lists and firmware from supported vendor portals into a central facility repository.

Isolated OT preparation

Make selected content available through Enterprise and OT Upstream workflows; OT initiates configured interval checks.

Controlled offline handoff

Prepare the approved content for manual external-media import when the OT environment is disconnected.

MINIMUM DEPLOYMENT RESOURCES

CPU	RAM	STORAGE
4 vCPU	**16 GB minimum**	**500 GB SSD minimum**

Upstream: 500 GB minimum, or 1 TB for multilingual content. Linux local repositories: at least 1 TB per Linux vendor type. Expand capacity for retained content and vendor versions.

Windows Server x64 / IIS / PostgreSQL

BUILT FOR CRITICAL INFRASTRUCTURE

Oil & gas · Energy & utilities · Manufacturing · Water · Smart cities · Transport

Explore your deployment with REPLIL.

replil.com / sales@replil.com