REPLIL™
INDUSTRIAL PATCH MANAGER

REPLIL INDUSTRIAL PATCH MANAGER (IPM)

Unified OT Patch & Firmware Management for Critical OT Environments

sales@replil.com

POWERED BY AI

INTRODUCTION

REPLIL IPM is a purpose-built **agentless patch and firmware management solution** designed for **Industrial Control Systems (ICS)** and **Operational Technology (OT)** networks. It simplifies and secures patching across **automation vendors, operating systems, network firmware, and Level 1 assets (PLCs, controllers)**—ensuring **compliance, availability, and cyber resilience** in highly sensitive environments.

- **Unified Console –** A single centralized view of all nodes, software's, WSUS servers, and distributed critical infrastructures.
- **End-to-End Monitoring –** Customers can see patch health, performance metrics, and vulnerability exposure across the entire OT/IT landscape.
- **Critical Patch Awareness –** Easily identify systems with missing critical patches or vendor-validated patches requiring urgent action.
- **Automation Vendor Baselines –** Validate compliance against automation vendor–approved patch sets (Any Automation Vendor).
- **Performance Impact Analysis –** Quickly detect performance bottlenecks, outdated assets, and vulnerable nodes.
- **Scalable Visibility –** From a single site to multi-site deployments, all data is consolidated into one intuitive interface.
- **Actionable Reporting –** Generate KPI dashboards, approval history, and vulnerability state reports to support governance and compliance.

BUILT FOR OT REPLIL UNIFIED PATCH MANAGEMENT

(AGENTLESS. VALIDATED. TRUSTED FOR CRITICAL INFRASTRUCTURE.)

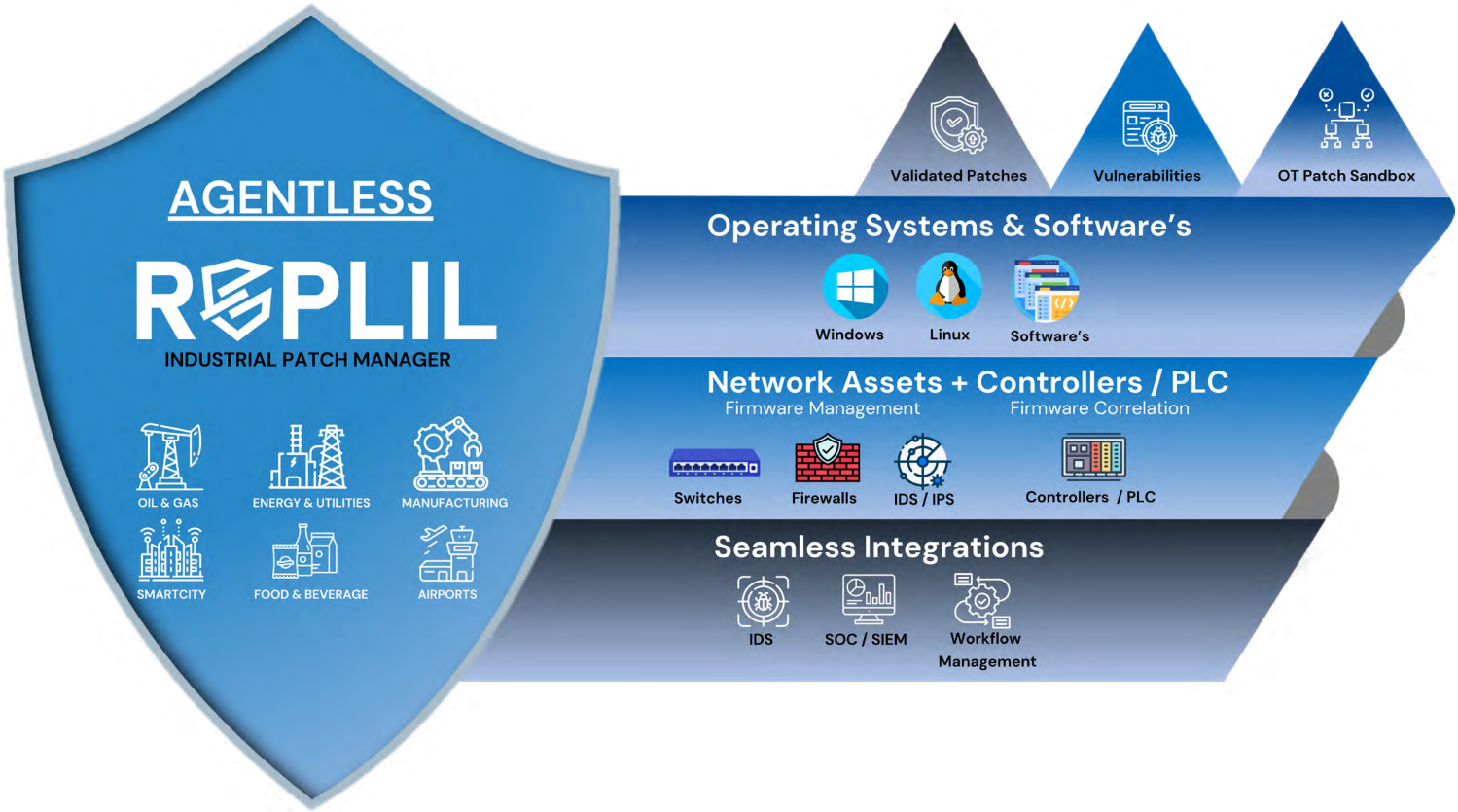
REPLIL delivers a unified, agentless patch management platform purpose-built for OT — simplifying compliance, reducing risk, and ensuring operational continuity across all layers of critical infrastructure.

- **Unified Visibility Across OT Zones**
  (Complete ecosystem insight)
- **Agentless by Design**
  (Seamless integration with existing systems)
- **OEM-Validated Patches**
  (End-to-end visibility & analysis)
- **Air-Gapped Patch Capability**
  (1st in class for isolated networks)
- **Integrated Performance Impact Analysis**
  (Eliminates data silos)
- **Advanced OT Patch Sandbox (OPS)**
  (Test before deploy)

SIMPLIFYING PATCH MANAGEMENT IN COMPLEX ICS ENVIRONMENTS

Industrial Control Systems (ICS) operate within multi-vendor ecosystems, often involving 10–15 or more vendors across software, network assets, operating systems, and cybersecurity solutions.

REPLIL Industrial Patch Manager (IPM) redefines this complexity by delivering a unified, agentless, and secure approach to patch management—purpose-built for critical infrastructure and OT networks.



REPLIL™
INDUSTRIAL PATCH MANAGER

OT Validated Patches
Streamline Industrial Patch Management From Any OT (ICS) Automation Vendors. Automate Correlation for Effortless Administration.

Multi-Automation Servers Management
Identify, Validate, Manage Multiple Patch Management Server (Native API, REPLIL Client)

Agentless Design
Agentless Approach Inline to Multi-Automation Vendors Patch Management Designs and Strategy.

Compliance
Meet Major Industry Compliance Standards (IEC 62443-2-3 / NCA / NERC / NIST etc.)

Sandbox (Test & Approve)
Automated Testing of Single Patch or Multiple Automation Validated Patches in an Isolated Sandbox Environment.

Baseline Management
Identify Any Discrepancies From Installed OS, Applications, Components and Network Devices Configuration.

Vulnerability Management
Passive Vulnerability Mapping against the OS, Application & Identified Patches to Prioritize Based on Criticality.

SOC / SIEM Visibility
Get Enhanced Visibility of Validated Patches in SOC for Different Automation Vendors.

Artificial Intelligence (AI) Powered
Automatically Troubleshoot and Resolve The Issues Identified In the Patch Management Infrastructure.

Customized Reporting
Drag & Drop Report Builder with Endless Possibilities, C-Level to Detailed Reports in 10+ different Formats.

Analytical Dashboards
Advanced Analytical Status and Dashboards for Key Patch Management Factors.

IEC62443-2-3 Workflow
Incorporating The IEC62443-2-3 Recommendations & Workflows to reduce the gap in Industrial Patch Management.

1. **Industrial Focus:** Tailored specifically for critical infrastructures, REPLIL IPM addresses the unique challenges faced by industries operating multiple automation vendors.
2. **Artificial Intelligence Integration:** Harnessing the power of Artificial Intelligence, REPLIL IPM brings predictive capabilities to patch management, optimizing deployment strategies and minimizing vulnerabilities.
3. **Rapid Deployment:** Minimize patch deployment time and distribution efforts with REPLIL IPM's streamlined processes and automated workflows, ensuring swift response to emerging threats.
4. **Enhanced Visibility:** Gain comprehensive visibility into validated and approved patches, empowering administrators with the knowledge needed to make informed decisions regarding patch application.
5. **Real-Time Monitoring:** Monitor the patch status of facilities in real-time, ensuring that security postures remain up-to-date and resilient against potential cyber threats.
6. **Efficient Assessment and Maintenance:** Simplify the assessment, management, and maintenance of patches with REPLIL IPM's centralized platform, reducing administrative burdens and enhancing overall system reliability.
7. **Integration with SIEM:** Seamlessly integrate with Security Information and Event Management (SIEM) systems to provide centralized posture visibility, enabling organizations to proactively identify and respond to security incidents.

REPLIL™
INDUSTRIAL PATCH MANAGER

BENEFITS

- **Enhanced Security:** Mitigate the risk of cyber threats by ensuring timely patch deployment and maintaining an up-to-date security posture across critical infrastructures.
- **Operational Efficiency:** Streamline patch management processes to reduce downtime and optimize operational efficiency, enabling organizations to focus on core business objectives.
- **Compliance Assurance:** Facilitate compliance with industry regulations and standards by maintaining a comprehensive record of patch activities and security postures.
- **Cost Savings:** Minimize the financial impact of security breaches and system vulnerabilities by proactively managing patches and reducing the likelihood of cyber attacks.

WHY REPLIL IPM?

Unlike generic patch tools, REPLIL IPM is engineered for **the unique challenges of OT**:

- Integrate with **existing patch management solutions** or use built-in **agentless patch management**
- Operates in **restricted, air-gapped networks**.
- Understands **industrial vendor patch cycles**.
- Provides **visibility across IT, OT, and Level 1 devices** in one platform.

Centralized Patch management of distributed environments — Windows, Network, Linux, and Level 1 assets — to speed up patching and compliance

CERTIFICATIONS:

- IEC62443-4-1 (Secure by Design)
- IEC62443-4-2 (SL3 Compliant)
- ISO 27001

DEPLOYMENT MODELS

On-Premises

Hybrid

EXPERIENCE REPLIL IPM IN ACTION

Request a Live Demo
sales@replil.com