REPLIL

Worlds 1st Real-time

Industrial Patch Manager

FEATURES

Validated Patches by ICS Vendors

Distribute validated approved patches to different plants and sites. Deploy, manage and assess the patches.

Enhanced (SOC) visibility

Identify missing, validated and approved patches to fine-tune the SOC for the latest threats and actions.

Cybersecurity Devices Signatures

Deliver signature updates for IPS / IDS and Antivirus engines to protect against latest threats.

Manage 3rd Party Patches

Quickly identify the out-of-support applications and update using multiple methods.

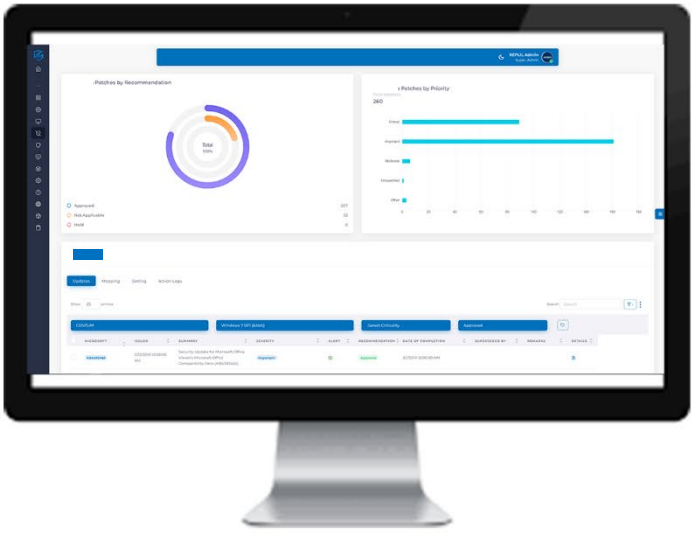
Centralized Patches View (360)

Centralized visibility of missing / approved / validated patches. No more single automation vendor monitoring.

Compliance

Support in increasing the effiency of patch program by providing vendor agnostic view.

1. Missing & Approved Patches Visibility
2. Validated and Applicable Patches



INDUSTRIAL PATCH MANAGER (IPM)

Centralized Patch Management Solution for all major ICS Vendors.

Manage any OEM Patches, Identify missing approved patches from various industrial vendors, and manage centrally with a 360-degree view of full industrial assets and network devices patch status.

Call +1 805-742-4848 or visit www.replil.com

REPLIL

INDUSTRIAL PATCH MANAGER (IPM)

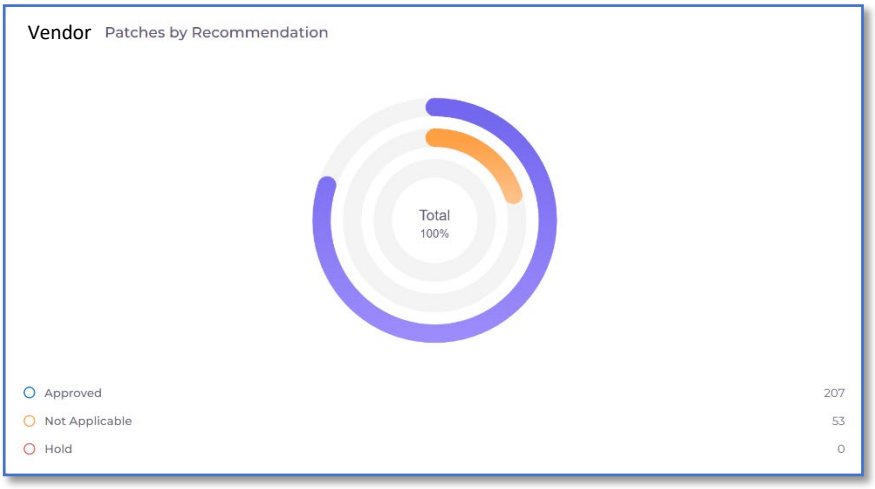
DATASHEET

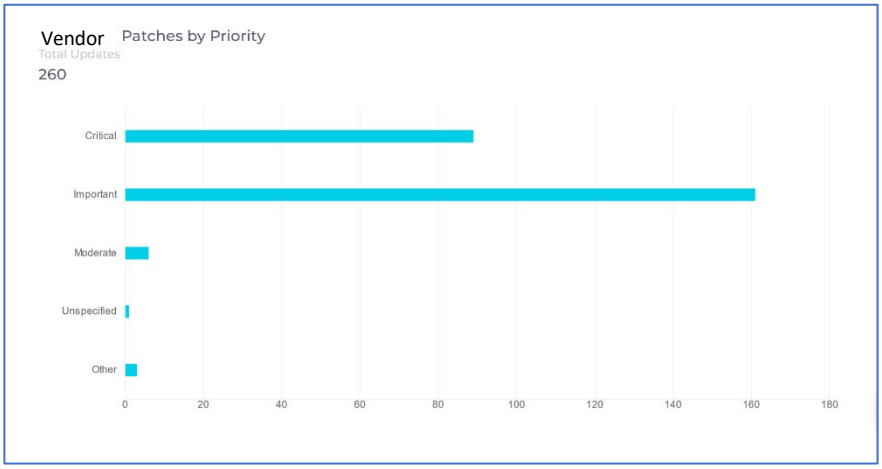
www.replil.com

Patches by Automation Vendor Recommendation

REPLIL IPM provides enhanced information of recommendations as per automation vendors not as per Microsoft ®

- Validated patches by Automation vendor
- Approved for install
- Not Applicable patches
- On-Hold patches by Automation Vendor



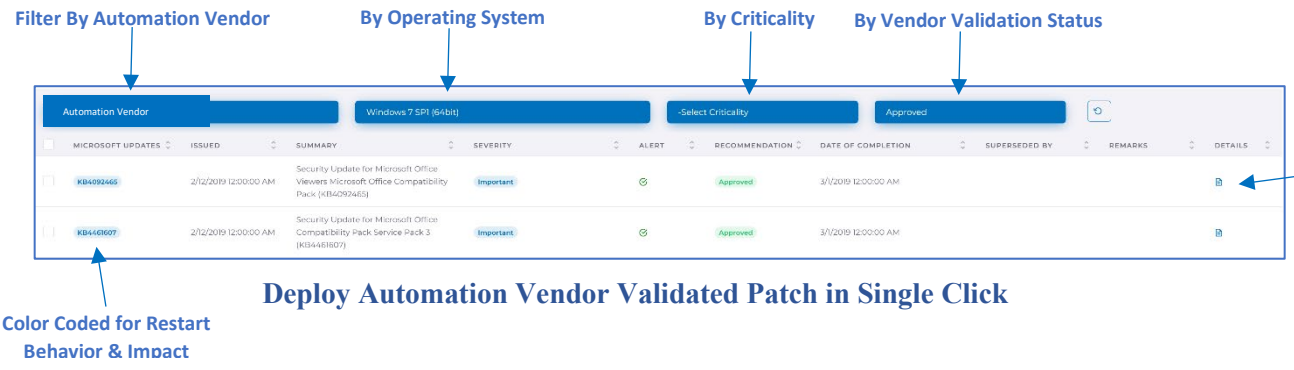


Patches by Automation Vendor Criticality

Get visibility of criticality of different patches validated by automation vendors.

- Critical Patches (High-Priority)
- Important Patches
- Moderate Patches

Filter by Criticality or by Automation vendor DCS system.



Deploy Automation Vendor Validated Patch in Single Click

Call +1 805-742-4848 or visit www.replil.com

REPLIL

INDUSTRIAL PATCH MANAGER (IPM)

DATASHEET

www.replil.com

Supported Vendors

IPM supports multi-vendor environments and easily expands to support additional vendors environments, our integration possibilities are endless. With a fully customizable software our offerings are fine-tunned to our customer's needs.

We support with our continuous growing integration portfolio

- Any automation vendor patches (DCS Providers, Historian Systems, Safety System Providers, Industrial IOT etc.)
- Microsoft ®
- 3rd Party Patches (Industrial Application / Non-Microsoft Patches)
- Networking vendors
- Security vendors (IPS / IDS Engines / Validated Antivirus Updates)

Deployment Scenarios

REPLIL IPM can be deployed in various process environments

- Converged environment
- Isolated environments (protected by data diode / no-internet)

Compliance Summary

NERC Standard	*Requirement*	*REPLIL (IPM) Response*
CIP-007-6 R2 Part 2.1	A patch management process for tracking, evaluating, and installing cyber security patches for applicable cyber assets	IPM provides centralized management and compliance of multi-vendor environments and offers patch management lifecycle to ensure the attack surface is reduced.
CIP-007-6 R2 Part 2.2	At least once every 35 calendar days, evaluate security patches for applicability.	IPM Dashboard offers real-time required patches from Microsoft ® WSUS and approved patches by industrial vendors Yokogawa / Honeywell / Rockwell / Schneider etc.
CIP-007-6 R2 Part R2.3	For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: apply the applicable patches, create a dated mitigation plan or revise an existing mitigation plan	IPM offers auto-deployment and patch management lifecycle to identify the risks associated with the patch with 360-Degree view of complete environment.

Other supported standards

- IEC 62443
- NCA