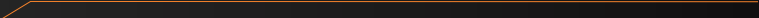




DATA SHEET • RISK SIGNAL™

Risk-Based Vulnerability Management For OT



Industrial Defender® is a leading source of OT asset data for protecting industrial operations and meeting compliance —providing deeper-level asset data, endpoint information, historical context, and change-monitoring capabilities across the OT environment.



RISK-BASED VULNERABILITY MANAGEMENT FOR OT

Patch what matters first. Move from awareness to action.

A premium playbook layer that turns your existing risk model into the next defensible move. Your vulnerability list grows faster than your maintenance window. You already know where risk lives — the hard part is deciding which patch or upgrade comes next, what effect it should have, and how to hand that decision off to operations without losing context.

Risk Signal™ is the action layer for that decision. It builds on your configured risk profile, vulnerability urgency, and patch and software inventory data to surface a small set of recommendations that produce the largest reduction in risk for the lowest operational effort. It then converts those recommendations into ordered playbooks that publish directly into work packages — closing the loop from insight to execution.

01 One Workflow, End to End				
STEP 01 Identify	STEP 02 Decide	STEP 03 Act	STEP 04 Monitor	STEP 05 Verify
Posture tiles, risk trend, and the highest-priority recommendations on a single landing view.	Compare patches and upgrades across four ranking lenses. Switch lenses without losing context.	Convert recommendations into an ordered playbook. Publish directly into work packages.	Track work status, generate reports, subscribe to summaries, drill into asset detail.	Compare current, simulated, and actual post-maintenance posture to confirm the change landed.

02 The Recommendation Workspace

Patch and software-upgrade recommendations are presented side by side, each ranked by expected impact and effort. Switch lenses to optimize for what matters in this maintenance window.

Most Risk Reduced Largest weighted drop in overall risk score across the affected fleet.
Most CVEs Fixed Highest count of CVEs retired in a single action.
Most Assets Improved Broadest reach across critical and non-critical assets.
Oldest Vulnerabilities Targets long-lived findings that have aged past your tolerance.

TOP PATCH RECOMMENDATIONS · MOST RISK REDUCED

01	KB5034441 · Windows 10 LTSC 14 critical assets · 3 CVEs · 87 d old	–18.4%
02	Schneider EcoStruxure 2024.1 9 critical assets · 5 CVEs · 41 d old	–12.1%
03	Rockwell FactoryTalk 7.32 22 assets · 2 CVEs · 152 d old	–9.6%
04	OpenSSL 3.0.13 backport 61 assets · 4 CVEs · 19 d old	–7.3%

HIGH-RISK ASSETS
248 ▶ **161**

EFFORT SCORE
Low 3 of 5

03 The Decision Model

INPUTS

Your existing risk model

Risk Signal™ inherits your assigned risk profile and risk factors. There is no second risk system to configure or reconcile.

OPTIMIZE FOR

Risk reduction over effort

Each recommendation balances projected risk reduction against effort — affected assets, critical assets, and patch age.

OUTPUT

Explainable, defensible

Every ranking shows what it fixes, who it affects, what risk bands should change, and the work artifact it produces.

04 What-If Simulation

CURRENT POSTURE



◆ Critical ◆ High ◆ Medium ◆ Low

AFTER PLAYBOOK (PATCHES + UPGRADES)



▼ 78% reduction in critical & high-risk assets

05 Capabilities & Benefits

001

Personalized risk foundation

Built on your assigned risk profile and risk factors — no second risk model to reconcile.

002

Ranked recommendations

Switch between four lenses: most risk reduced, most CVEs fixed, most assets improved, oldest open.

003

Effort-aware ranking

Effort signal accounts for affected assets, critical-asset count, and the age of the patch or upgrade.

004

Upgrade-path guidance

Minimal, best, and safest target-version recommendations where upgrade data is available.

005

Playbook generation

Convert recommendations into an ordered, scoped action plan — first, second, third.

006

Work-package handoff

Publish or seed playbooks directly into Work Automation; nothing ends as a passive list.

007

What-if simulation

Compare current posture, projected post-action, and actual post-maintenance results.

008

Reporting & subscriptions

Generate reports from any playbook, schedule subscriptions, and drill into related asset views.

**Stop triaging the list.
Start running the play.**

Risk Signal™ turns your configured risk model into a defensible patching plan that publishes straight into operations — with the before, after, and verified outcome attached.

[SCHEDULE A DEMO ▶](#)

THE INDUSTRIAL DEFENDER® DIFFERENCE

Since 2006, Industrial Defender® has been solving the challenge of safely collecting, monitoring, and managing OT asset data at scale, while providing cross-functional teams with a unified view of security. Their specialized solution is tailored to complex industrial control system environments by engineers with decades of hands-on OT experience. Easy integrations into the broader security and enterprise ecosystem empower IT teams with the same visibility, access, and situational awareness that they're accustomed to on corporate networks. They secure some of the largest critical control system deployments with vendors such as GE, Honeywell, ABB, Siemens, Schneider Electric, Yokogawa and others to protect the availability and safety of these systems, simplify standards and regulatory requirements, and unite OT and IT teams.

Planning an OT Security Project?

[SCHEDULE A DEMO](#)

FOR MORE INFORMATION

1 (877) 943-3363 • (617) 675-4206 • info@industrialdefender.com

225 Foxborough Blvd, Foxborough, MA 02035

industrialdefender.com

© 2026 Industrial Defender®. All Rights Reserved.

