



# FLOWFORT

---

## PLATFORM



### INDUSTRIAL RISK & PATCH MANAGEMENT

FlowFort is an OT-native Patch, Risk, and Compliance platform designed to act as the operational control plane for OT security. It consolidates asset context, physical location, patch intelligence, risk treatment, and compliance evidence into a single system of record, enabling organizations to move from detection to defensible action.



## THE CHALLENGES

OT environments today face several growing challenges, including increased connectivity to enterprise IT and cloud systems, higher exposure to ransomware and supply chain attacks, aging systems that are difficult to patch, and stricter regulatory requirements such as IEC 62443 and NIST CSF. **Traditional IT security models do not work well in OT**, where availability, safety, and operational stability are more important than quick fixes, making risk decisions more complex. As a result, OT security is no longer just about identifying devices, but about managing risk across operations, maintenance, and compliance.



## THE SOLUTION

**FlowFort** applies proven industrial safety and reliability principles to cybersecurity, bringing structure, ownership, and consistency to risk decisions. It integrates outputs from OT detection tools with operational, physical, and governance data to create a unified decision layer. By combining asset context, vulnerabilities, and risk aligned to operational impact, **FlowFort enables consistent risk management and serves as a central system of record for OT cyber risk.**



## KEY CAPABILITIES

- Asset Discovery & Inventory
- OT Network Monitoring
- Risk-Based Vulnerability Management
- Intelligence-Driven Threat Detection
- Patches priority & Compliance Management
- Clear Dashboard Visuals for Data Analysis
- Dynamic Approval Flows
- KB-Specified Monitoring & Relations



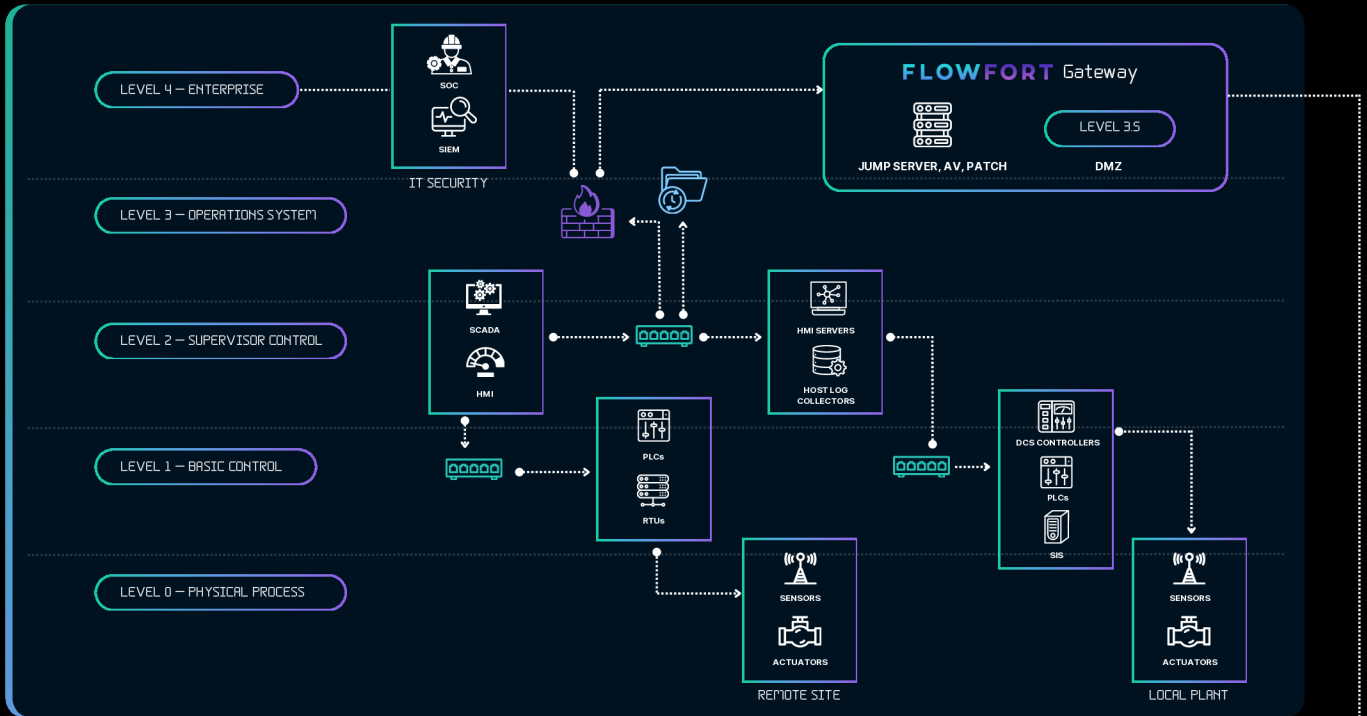
## WHY FLOWFORT?

- ✓ **Beyond Detection**  
We enable remediation by managing safe patch deployment with KB-based validation, unlike platforms that only handle detection.
- ✓ **KB-Specified Prioritization**  
Patches are validated against vendor KBs to reduce risky or unsupported installs.
- ✓ **Operational Safety First**  
Risk scores combine Business Impact, Process Impact, Exposure, and Purdue Level to minimize downtime.
- ✓ **Governed Approval Flows**  
Approver/reviewer roles ensure accountable decisions and compliance traceability.



# THE FLOWFORT SYSTEM ARCHITECTURE

PURDUE MODEL



DATA SOURCE 1

**Network Discovery & Passive Monitoring**

- tenable
- DRAGOS
- NOZOMI NETWORKS
- CLAROTY

DATA SOURCE 2

**Patch Management**

- WSUS

DATA SOURCE 3

- OEM Advisory
- ICS Advisories
- Threat Intelligence
- Offline Asset Inventory

**FLOWFORT**

**Unified Automation & Orchestration Layer**

- Asset Inventory
- Patch Intelligence
- Risk Governance
- Compliance Reporting

**Stakeholders Outputs**

- CISO Dashboards
- Auditor Reports
- Operations Workflows

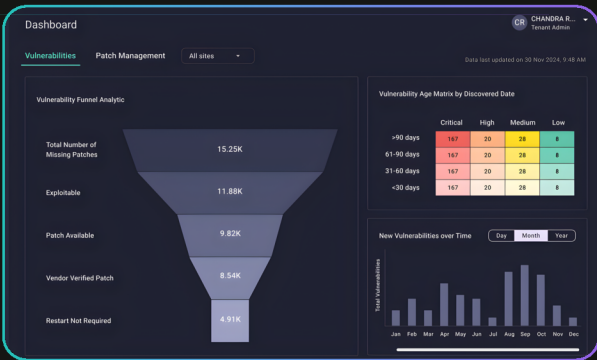
**Workflow Outputs**

- splunk >
- Microsoft Sentinel
- Radar
- Google SecOps



## KEY FEATURES

### Vulnerability Funnel Analytic



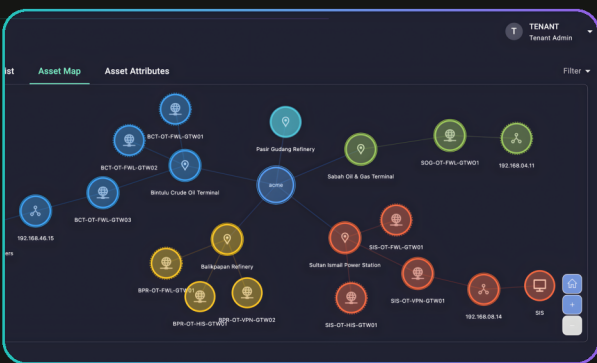
Transforms thousands of missing patches into clear, risk-based actions. **Prioritizes vendor-verified and critical fixes** to speed up decisions, reduce downtime, and strengthen OT security.

### Asset Attributes

ATTRIBUTE	VALUE	SCORE	WEIGHT(%)
Threat Intel	Actively Exploited/Zero Day, High Exploitability, Medium Exploitability, Low Exploitability, No Known Exploit	5, 4, 3, 2, 1	20
Business Impact	Extensive, Moderate, Significant, Minor, Negligible	5, 3, 4, 2, 1	15
Process Impact	No Disruption, Critical Disruption, Moderate Disruption, Major Disruption, Minor Disruption	1, 5, 3, 4, 2	20
Purdue Level	Level 0, Level 1, Level 2, Level 3, Level 4	5, 4, 3, 2, 1	25
Exposure	Segmented Network, Isolated, Internet Facing, DMZ Exposure, Internal Network, Critical Zone	2, 1, 4, 4, 3	20

Calculates patch priority using key **asset and risk factors** such as business impact, exposure, and Purdue level to help focus on the most critical updates.

### Asset Inventory



Collects and visualizes data automatically, consolidating asset details, vulnerabilities, criticality scores, and related KBs and CVEs for a **complete operational overview**.

### Risk Management

RISK TITLE	KB NAME	RISK RATING	LIKELIHOOD	IMPACT	RISK LOG	CHOSEN STRATEGY
Unauthorized Administrative Access Risk- Windows 2019	KB4598480	Medium	Probable	Tolerable	📄	Mitigation Acknowledgment
Unrestricted Network Access to OT Resources	KB5037036	Low	Rare	Acceptable	📄	Review
Unpatched PLC Vulnerability (CVE-2023-12345) in Refinery Control System	KB4562562	Medium	Unlikely	Tolerable	📄	Review
Outdated PLC Firmware Exposing Critical Manufacturing Line	KB4052623	High	Rare	Acceptable	📄	Review
Control System Downtime	KB5029379	High	Possible	Tolerable	📄	Review
Weak Firewall Rules Allowing Insecure Protocols	KB5029379	Medium	Possible	Significant	📄	Review
Outdated PLC Firmware Exposing Critical Manufacturing Line	KB4601393	High	Unlikely	Significant	📄	Review

Applies clear strategies to handle risks while assigning approver and reviewer roles for **accountability, compliance, and informed decision-making**.



## KEY FEATURES

### Vulnerabilities

CVE	NAME	CVSS SCORE	EXPLOITABLE	AFFECTED
CVE-2019-0545	An information disclosure vulnerability exists in .NET Framework and .NET Core which allows bypassing Cross-origin Resource Sharing (CORS) configurations, aka ".NET Framework Information Disclosure."	7.5	Yes	1
CVE-2024-21410	Microsoft Exchange Server Elevation of Privilege Vulnerability	9.8	Yes	18
CVE-2024-21409	A security feature bypass vulnerability exists in secure boot, aka Microsoft Secure Boot Security Feature Bypass Vulnerability.	9.6	Yes	5
CVE-2022-41064	.NET Framework Information Disclosure Vulnerability	5.8	Yes	1
CVE-2023-21528	Microsoft SQL Server Remote Code Execution Vulnerability	7.8	Yes	1
CVE-2023-21704	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	7.8	Yes	1
CVE-2023-21705	Microsoft SQL Server Remote Code Execution Vulnerability	8.8	Yes	1
CVE-2023-21713	Microsoft SQL Server Remote Code Execution Vulnerability	8.8	Yes	1
CVE-2023-21718	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	7.8	Yes	1

Displays each vulnerability with its affected systems, KBs, vendors, and installation status, allowing teams to **identify and remediate high-risk issues efficiently.**

### Patch Management

**Knowledge Base Verification**

Vendor Type: **Global Vendor** / Tenant Vendor

Vendor Name: Rockwell Automation  
 Product: FT Remote Access  
 Version: 14.2.0  
 Operating System: Linux  
 OEM Qualification Date: 2025-09-17

Evidence:  
 Reference: <https://www.rockwellautomation.com/en-gb/ota/factorytalk-https://connectibility.rockwellautomation.com/>  
 Email Proof: [http://pcme.backendstaging.attackbox.online/media/KB\\_v\\_](http://pcme.backendstaging.attackbox.online/media/KB_v_)  
 Comments: Safe to deploy in production environment

**Installs only verified patches** to maintain stability and prevent outages, ensuring critical infrastructure remains secure and uninterrupted.

### Risk Mitigation Action Flow

**Risk Mitigation Actions**

Filters: Pending(22) | Acknowledged (12) | Implemented (5) | Deferred (3) | TBD (3)

Grid of Action Cards (Example):

- Implement Intrusion Detection and Prevention Systems (IDS/IPS)
- Implemented by: tenantanalyst@gmail.com
- Target Date: 12-07-2023
- View Details

Guides **every mitigation step** from planning to implementation, tracking outcomes for full visibility and operational transparency.


## ALL IN 1 OT SECURITY OPERATIONAL CONTROL PLANE

- Detection context from OT security tools
- Physical context from floor plans and rack layouts
- Patch and vulnerability context from WSUS and OEMs
- Risk context aligned to industrial impact
- Governance context aligned to enterprise risk management




# COMPREHENSIVE ASSET VISIBILITY: LOGICAL AND PHYSICAL


## Logical Context




Sites, plants, substations, and facilities



Purdue levels (LO-L5)




System groups (DCS, SCADA, SIS, Historian, Substations)




Business functions and criticality


## Physical Context




Upload and management of floor plans



Visual placement of assets across locations



Mapping of assets to racks and RU positions



Precise asset identification down to rack level



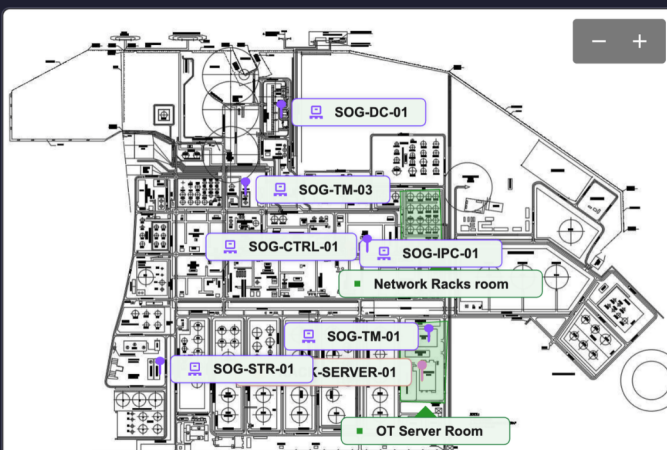
# LOCATION DIRECTORY

Location Directory
TA TENANT  
Tenant Admin

Search Sites, Buildings, Floors... Add

- ▶ Sultan Ismail Power Station
- ▶ Bintulu Crude Oil Terminal
- ▶ Sabah Oil & Gas Terminal
- ▶ Central Control Building
  - ▶ Server room
    - ▶ Network Racks room
    - ▶ OT Server Room
    - ▶ RTU Holder
    - ▶ SOG-DC-01
    - ▶ SOG-IPC-01
    - ▶ SOG-TM-03
    - ▶ SOG-STR-01
    - ▶ SOG-CTRL-01
    - ▶ SOG-SRV-02
    - ▶ SOG-SRV-03
    - ▶ SOG-STR-02
    - ▶ SOG-SRV-01
    - ▶ SOG-FT-01
    - ▶ SOG-SRV-04
    - ▶ SOG-TM-02
- ▶ Balingian Power station
- ▶ Balikpapan Refinery

Floor Plan







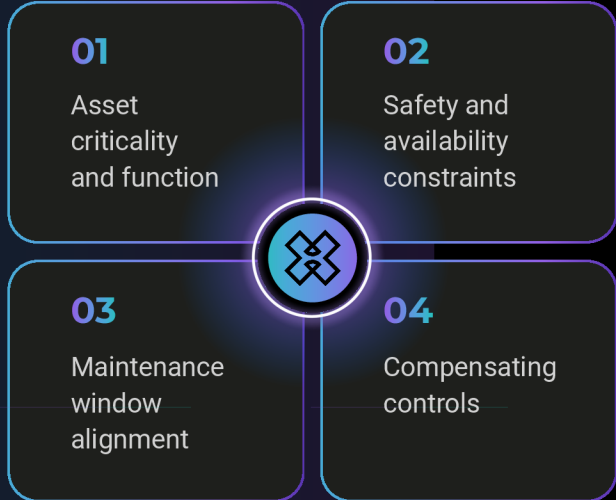
© 2026 FlowFort Powered by SecurePlex



## OT-AWARE PATCH INTELLIGENCE AND QUALIFICATION

Raw patch data alone is insufficient in OT environments. **FlowFort** transforms patch information into **actionable intelligence** meanwhile **patch decisions are evaluated**. This ensures that **patching decisions are risk-informed and operationally feasible, not purely CVSS- driven**.

-  Integrating with WSUS / SCCM to identify missing KBs
-  Enriching patches through automated KB-to-CVE correlation
-  Incorporating threat intelligence (exploit availability, weaponization)
-  Tracking OEM qualification and support status



## KEY DIFFERENTIATORS

- Designed specifically for OT operational realities
- Combines detection context with physical, business, and risk intelligence
- Moves organizations from visibility to governed action
- Reduces reliance on spreadsheets and manual audits
- Scales across multi-site, multi-tenant environments



## RACK DIAGRAM MANAGEMENT



- Import and repurpose existing rack diagrams
- Create and manage new rack layouts directly within the platform
- Support for mixed OT, IT, and network equipment racks
- Asset records
- Patch status
- Risk decisions
- Compliance controls



## STRUCTURED RISK MANAGEMENT FOR OT

FlowFort aligns OT cybersecurity with established industrial risk management practices, where risk is evaluated based on **consequence, exposure, vulnerability, and resilience**, not just technical severity.

### Risk Characterization

Each risk in FlowFort is tied to:

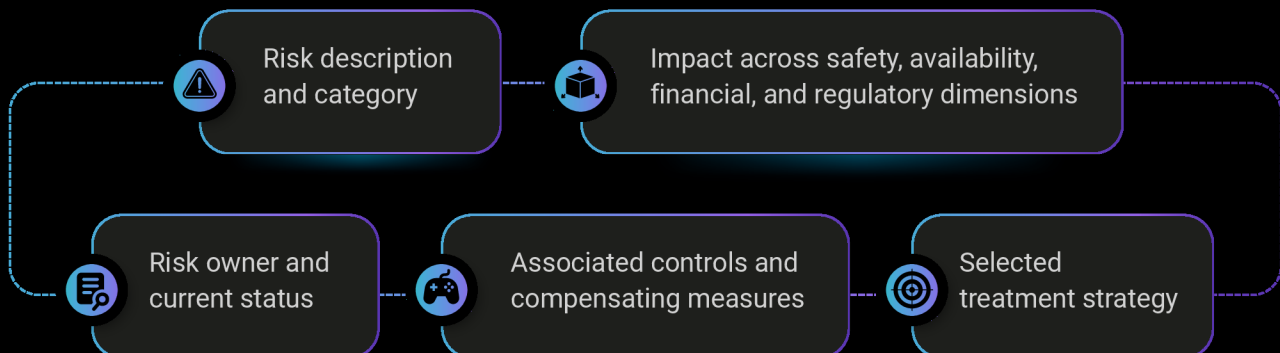
- Specific assets and system groups
- Operational and safety impact - Business continuity considerations
- Existing engineering and security controls



### Risk Treatment Strategies

- 01 Mitigate :**  
Reduce risk through technical or operational controls (patching, segmentation, monitoring, procedures)
- 02 Accept :**  
Acknowledge residual risk where mitigation is infeasible, with defined ownership, justification, and review timelines
- 03 Transfer :**  
Shift financial or operational risk through contracts, OEM responsibility, or insurance mechanisms
- 04 Avoid :**  
Eliminate risk by removing the exposure, such as decommissioning or redesigning systems

### Risk Register and Lifecycle





## COMPLIANCE EMBEDDED INTO OPERATIONS

**FlowFort** embeds compliance directly into operational workflows rather than treating it as an audit-only exercise. As a result, audits become faster, less disruptive, and evidence-driven.

### Supported Frameworks

IEC 62443 (zones, conduits, vulnerability and patch management)

NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover)

Internal cyber assurance and regulatory controls

### Evidence by Design

Automatic evidence capture from integrated systems

Analyst validation through attachments, screenshots, and references

Continuous compliance posture tracking



## OPERATIONAL WORKFLOWS ACROSS OT STAKEHOLDERS





## ABOUT FLOWFORT


FlowFort is built by OT security practitioners with deep experience across critical infrastructure, vulnerability management, red teaming, and compliance-driven environments. The platform reflects real-world constraints and bridges the gap between security visibility and operational execution.


Learn more about us here:


<https://secure-plex.com/flowfort>



Contact us:

 [query@secure-plex.com](mailto:query@secure-plex.com)

 +603-2242 4363

 Tower 2A, Avenue 5, The Horizon, Bangsar South, KL