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.

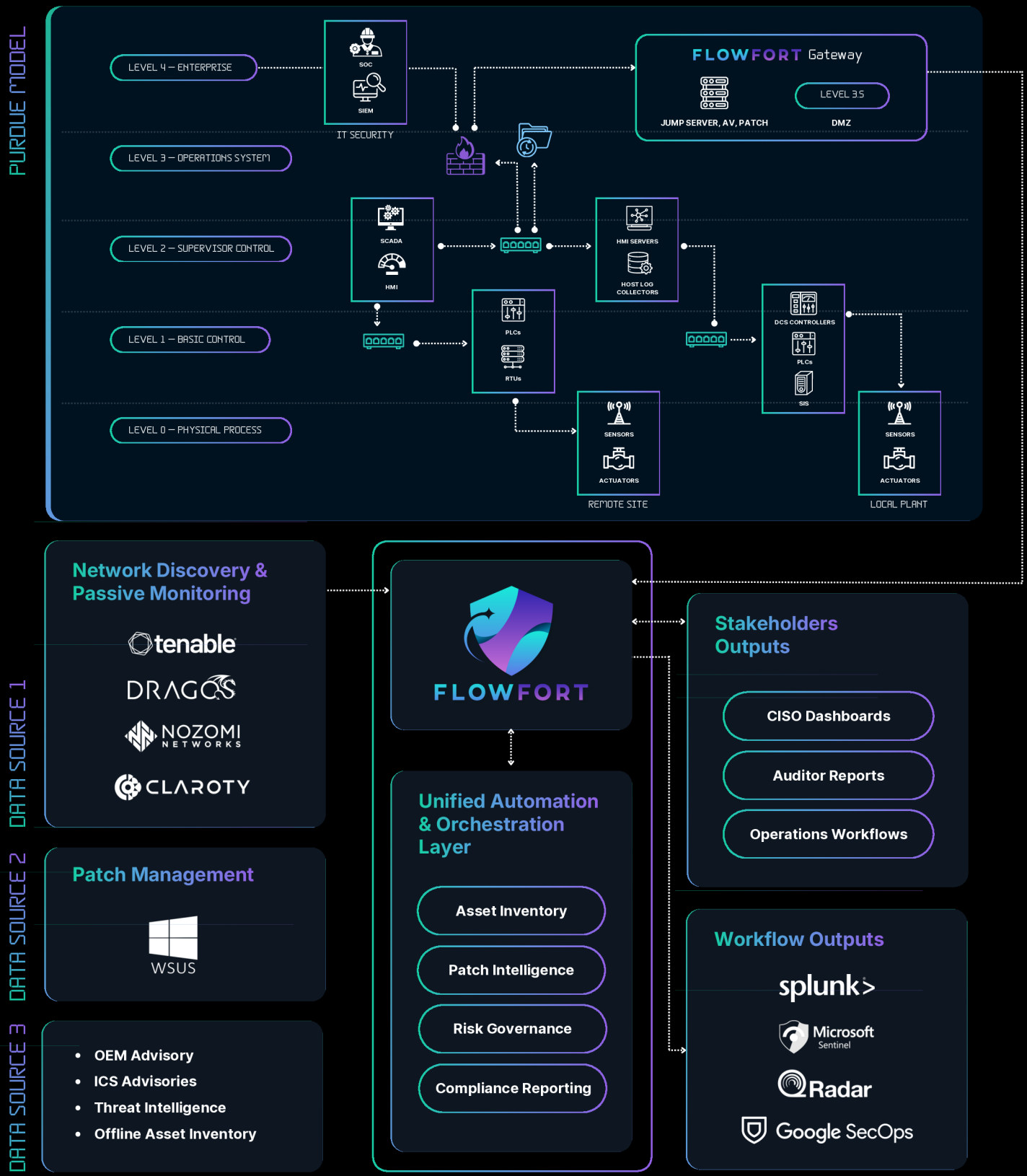
Operational Safety First

Risk scores combine Business Impact, Process Impact, Exposure, and Purdue Level to minimize downtime.

Governed Approval Flows

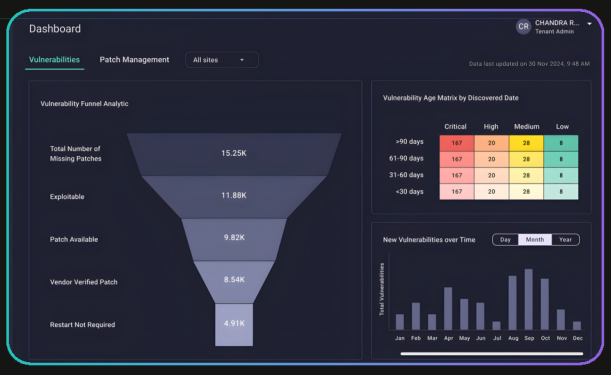
Approver/reviewer roles ensure accountable decisions and compliance traceability.

THE FLOWFORT SYSTEM ARCHITECTURE



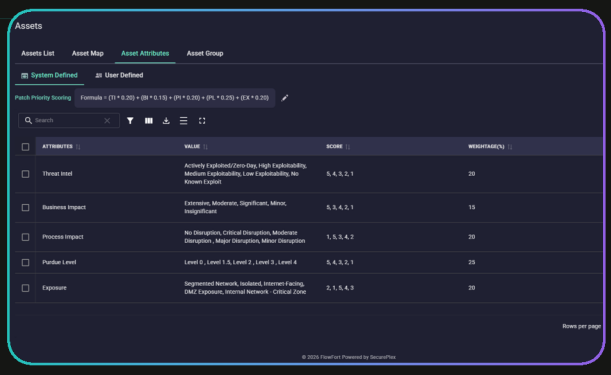
KEY FEATURES

Vulnerability Funnel Analytic



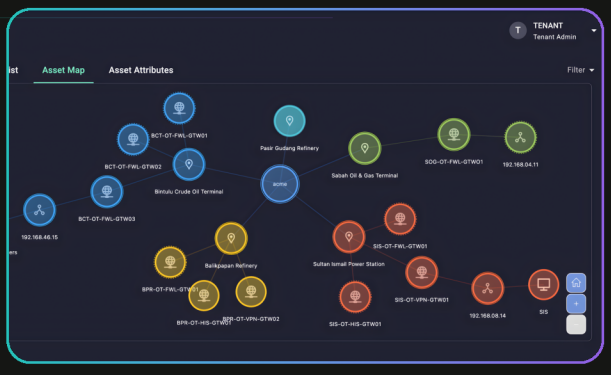
Transforms thousands of missing patches into clear, risk-based actions. **Prioritizes vendor-verified and critical fixes** to speed up decisions, reduce downtime, and strengthen OT security.

Asset Attributes



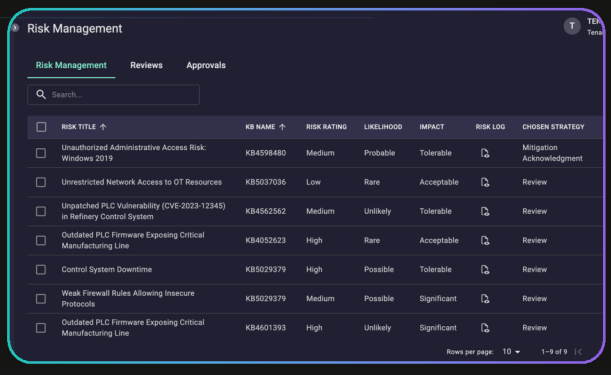
Calculates patch priority using key asset and risk factors such as business impact, exposure, and Purdue level to help focus on the most critical updates.

Asset Inventory



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

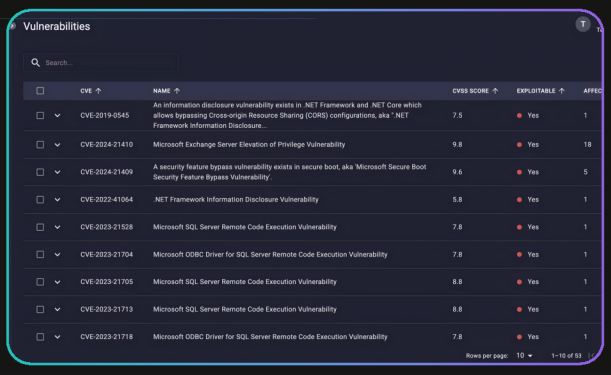
Risk Management



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

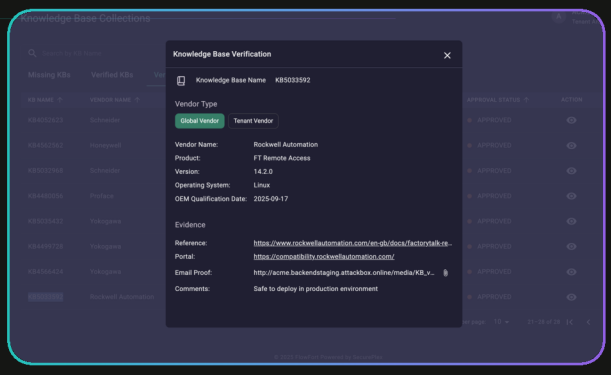
KEY FEATURES

Vulnerabilities



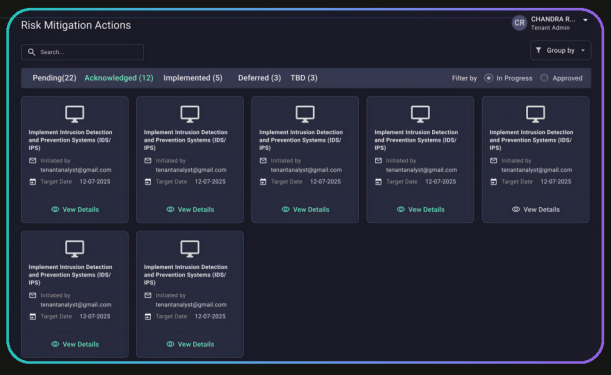
Displays each vulnerability with its affected systems, KBs, vendors, and installation status, allowing teams to **identify and remediate high-risk issues efficiently.**

Patch Management



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

Risk Mitigation Action Flow



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

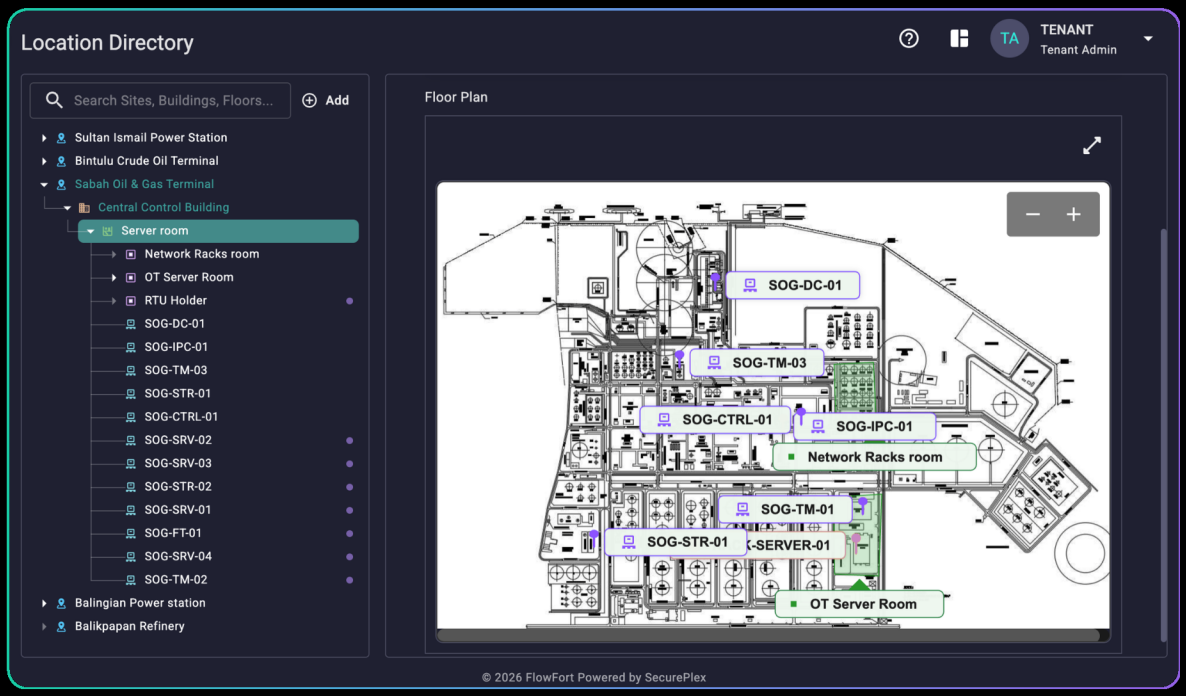
Logical Context

- Sites, plants, substations, and facilities
- Purdue levels (L0–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



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

01 Asset criticality and function

02 Safety and availability constraints

03 Maintenance window alignment

04 Compensating controls

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

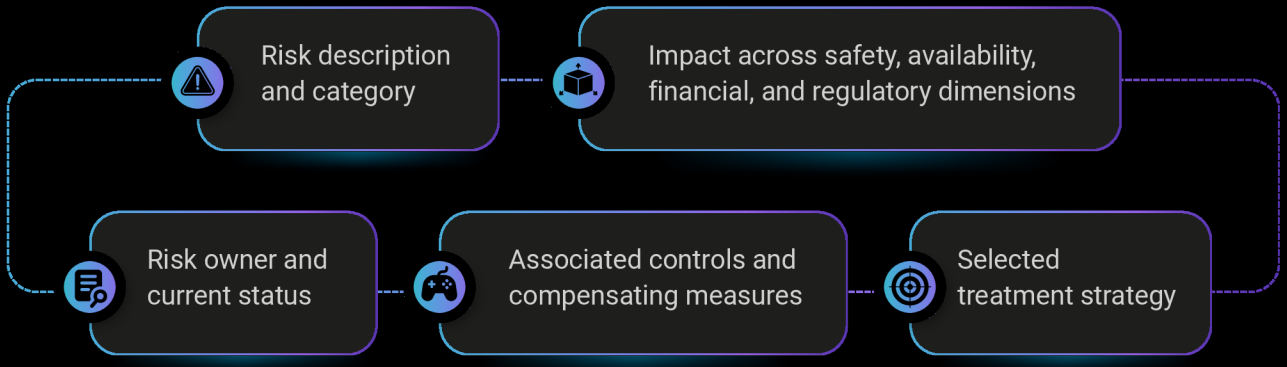
01 **Mitigate :**
Reduce risk through technical or operational controls (patching, segmentation, monitoring, procedures)

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

- OT engineering and maintenance teams
- Cybersecurity and risk teams
- Management and governance functions
- Internal and external auditors

Key Workflows

- Patch approvals
- Maintenance scheduling
- Risk acceptance
- Compliance attestation

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 +603-2242 4363 Tower 2A, Avenue 5, The Horizon, Bangsar South, KL