FLOWFORT

UNIFIED OT PATCH, RISK & COMPLIANCE MANAGEMENT

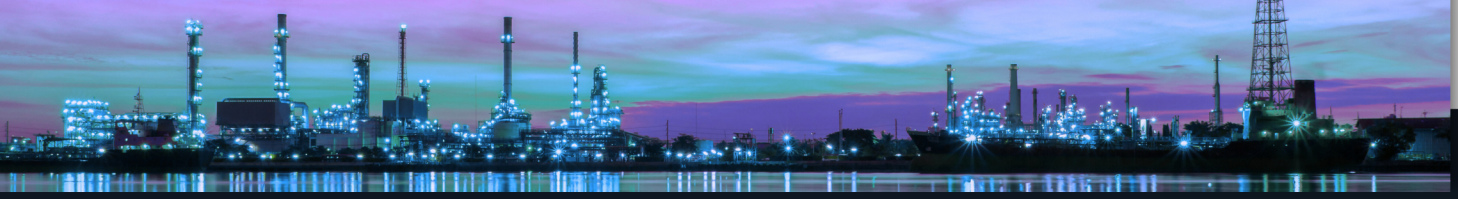
THE OPERATIONAL CONTROL PLANE FOR INDUSTRIAL CYBERSECURITY

AUTHOR

Sathish Kumar

Chief Technology & Product Officer
Secureplex, a Skill Quotient Group

APRIL, 2026



FROM VISIBILITY TO DEFENSIBLE ACTION

FlowFort is the *OT Cyber Operations Control Plane*

A unified platform for asset lifecycle management, location-aware risk governance, OT patch intelligence, and multi-framework compliance.

Built for the *world that exists after detection*

CONTENTS

FLOWFORT

The Missing Layer Between Detection & Defensible Decisions

The OT security industry has spent a decade solving the visibility problem. Detection platforms now identify assets, map protocols, and flag anomalies with remarkable accuracy. But a critical operational gap remains as most organizations cannot translate what they see into what they do with the governance, documentation, and operational rigor that regulators, boards, and plant operations teams demand.

Asset inventories remain trapped in Excel spreadsheets where physical locations are left blank and firmware versions are missing. Patching decisions are delayed or entirely unmanaged — 85% of organizations don't conduct regular OT patching. Risk acceptance is undocumented, unowned, and driven by audit cycles rather than operational reality. Compliance evidence is scattered across five or more disconnected systems.

FlowFort addresses this gap. It is an **OT-native Patch, Risk, and Compliance platform** designed to serve as the operational control plane for OT security, consolidating asset context, physical location, patch intelligence, risk treatment, maintenance state, and compliance evidence into a single system of record. FlowFort does not replace detection platforms. It absorbs their outputs and adds the governance layer that turns alerts into defensible decisions.

WHAT FLOWFORT IS AND WHAT IT IS NOT

FlowFort is **not** an OT detection platform, not a network detection and response (NDR) tool, not a vulnerability scanner, not a CMDB, and not a SIEM. Organizations that deploy Claroty, Nozomi, Dragos, or Tenable for detection and visibility should continue to do so, these platforms solve an essential problem. **FlowFort** is the ***operational decision layer that sits above detection tools***, governing **how the risks they surface are qualified, owned, treated, scheduled, and documented.** It is the system of record that answers "What did we do about it?" The question that detection platforms **were never designed to answer.**

This whitepaper examines the structural forces driving the need for post-discovery governance covering the threat landscape, the regulatory tsunami, and the market evolution, and details how FlowFort delivers capabilities that the current generation of OT security tools **was not designed to provide.**

85% of organizations don't conduct regular OT patching
TXOne / Frost & Sullivan 2024

52% of orgs now assign OT security to the CISO
Fortinet 2025

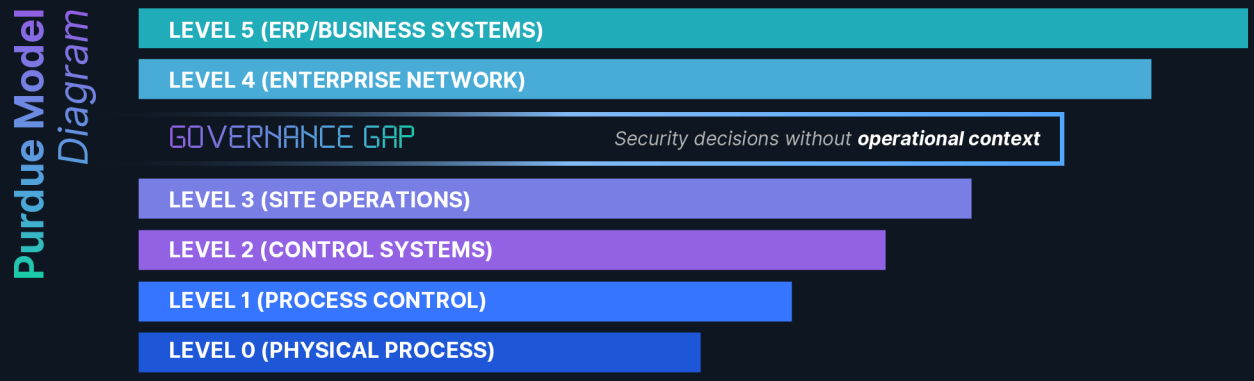
$50B+ projected OT security market by 2030
MarketsandMarkets

69 DAYS of organizations don't conduct regular OT patching
TXOne / Frost & Sullivan 2024

Why Detection Is No Longer Enough

The OT security market has matured rapidly. Gartner published its first Magic Quadrant for Cyber-Physical Systems (CPS) Protection Platforms in February 2025, evaluating 17 vendors, a milestone signaling the market's transition from niche to enterprise-grade. Gartner projects that by 2027, three-quarters of CPS-intensive organizations will source cybersecurity from CPS protection platforms, and nearly half will prioritize remediation capabilities as a key selection criterion.

Yet the threat landscape is accelerating. Manufacturing has been the top ransomware target for four years, with over 100 groups impacting thousands of industrial organizations in 2024–2025. About 75% of attacks caused partial OT shutdowns, while 25% led to complete shutdowns. Nation-state actors — Volt Typhoon, Sandworm, and BAUXITE — have also shown the ability to access and manipulate industrial control systems using common protocols and weak credentials.



Detection answers the first question. Operations needs the next five.

Modern detection platforms excel at the foundational questions: What devices exist? What protocols are in use? What vulnerabilities are visible? But across the Purdue model, from Level 0 instrumentation through Level 3 site operations, operational leaders need answers to higher-order questions that detection alone cannot provide:

THE FIVE UNANSWERED QUESTIONS

Where is this asset physically? Not its IP address — its building, floor, rack, and IEC 62443 zone. **What is its operational impact?** What process does it support, and what fails if it goes down? **Can it be patched safely?** Is there a maintenance window? Has the OEM qualified the update? **Who owns the risk?** Is there a named owner with documented treatment? **How is this decision auditable?** Can it survive regulatory scrutiny under NIS2, Act 854, or IEC 62443?

The SANS 2024 ICS/OT Survey highlights ongoing gaps: despite increased monitoring, many organizations still lack OT-specific response tools, certifications, and formal plans. Most remain at low maturity (Levels 1–2 under IEC 62443-2-1:2024) due to limited tooling, resulting in fragmented operations across multiple disconnected systems, an issue FlowFort is built to solve.

Compliance Demands Governance Tooling

A global wave of regulation now mandates risk governance, vulnerability handling, and compliance documentation that visibility tools alone cannot deliver. The message from every major jurisdiction is consistent: **Demonstrating that you can see the problem is no longer sufficient, you must demonstrate that you can govern the response.**

EU NIS2 Directive

Up to €10M or 2% global revenue

Effective October 2024. Mandates risk assessments, vulnerability management, and 24-hour incident reporting with personal executive liability.

Malaysia Cyber Security Act 2024

RM 500,000 + 10 years imprisonment

Covers 11 NCII sectors. Mandates annual risk assessments, biennial audits, and 6-hour incident reporting. Major national oil companies already pioneering IEC 62443 adoption.

NIST CSF 2.0 + SP 800-82r3

Framework (de facto baseline)

New "Govern" function centralizing cybersecurity governance. SP 800-82r3 provides 300+ pages of OT-specific control baselines.

IEC 62443 (2024–2025)

Certification & regulatory requirement

New 62443-2-1-2024 for asset owner security programs. Zone and conduit model remains the gold standard. Referenced by EU, ASEAN, and 20+ industries globally.

Singapore OT Masterplan 2024

Regulatory mandate for CII

Extends OT security beyond critical infrastructure. 14 OEMs committed to secure-by-deployment. The regional model for ASEAN.

CISA CPG 2.0

Voluntary (de facto baseline)

December 2025. Unified IT/OT goals. Requires documenting serial numbers, checksums, and digital certificates for OT verification.

SOUTHEAST ASIA REGULATORY ACCELERATION

Malaysia's Act 854 and Singapore's OT Masterplan represent a decisive shift in ASEAN regulatory posture. Indonesia's BSSN now requires 24-hour incident reporting, with a comprehensive Cybersecurity Law in the 2025 legislative pipeline. The ASEAN Regional CERT, launched October 2024, provides the first legally binding cross-border information-sharing mechanism. For industrial operators managing refineries, palm oil mills, power stations, and mining sites across the region, compliance is no longer hypothetical, it is enforceable, immediate, and escalating.

From Detection Era to Governance Era

OT cybersecurity is undergoing a generational shift. The first era (2010–2020) was defined by the air-gap assumption and perimeter defense. The second era (2020–2025) was defined by asset discovery and network monitoring, the era of "see everything." The third era, now emerging, is defined by post-discovery governance: the ability to act on what you see, document what you decided, and prove compliance under audit.

This evolution is not a critique of detection-era platforms, they solved an essential problem and continue to provide foundational capabilities. The shift is driven by external forces that have changed what "adequate security" means: NIS2 requires demonstrated risk governance, NIST CSF 2.0 added Govern as a core function, IEC 62443-2-1:2024 mandates structured asset owner security programs, and CISOs, now responsible for OT security in 52% of organizations, up from 16% in 2022, need board-level reporting that detection tools were never designed to produce.

OT Security Maturity *Staircase*

Fortinet 2025 data shows only 46% reach Level 4

Three Structural Gaps Define The Transition

The patch governance gap. OT patching is far more complex than IT, requiring OEM validation that can take months, especially for legacy systems not designed for updates. While detection tools identify missing patches and WSUS distributes them, neither supports the full process—qualification, approval, scheduling, and documentation. As a result, 85% of organizations don't patch regularly, and those that do rely on ad-hoc processes.

The risk ownership gap. Every detection platform offers risk scoring. None provide formal risk registers with treatment workflows, named ownership, multi-step approval routing, and board-level reporting. Accountability for OT risk spans security, operations, engineering, and compliance — and this fragmentation leads to undocumented risk acceptance, decision paralysis, and disorganized incident response. When the board asks "What is our OT risk posture?", the CISO has a detection dashboard, not a governed risk program.

The physical context gap. Detection tools produce network topology maps. They show logical relationships between devices, IP addresses, protocols, traffic patterns. But as OT practitioners consistently report from the field: the network diagram shows logical structure; the actual physical location of assets remains unknown. During an incident, you need to know which building, which floor, which rack, which safety zone, not which subnet. No major detection platform provides this capability.

THE GOVERNANCE LAYER GAP

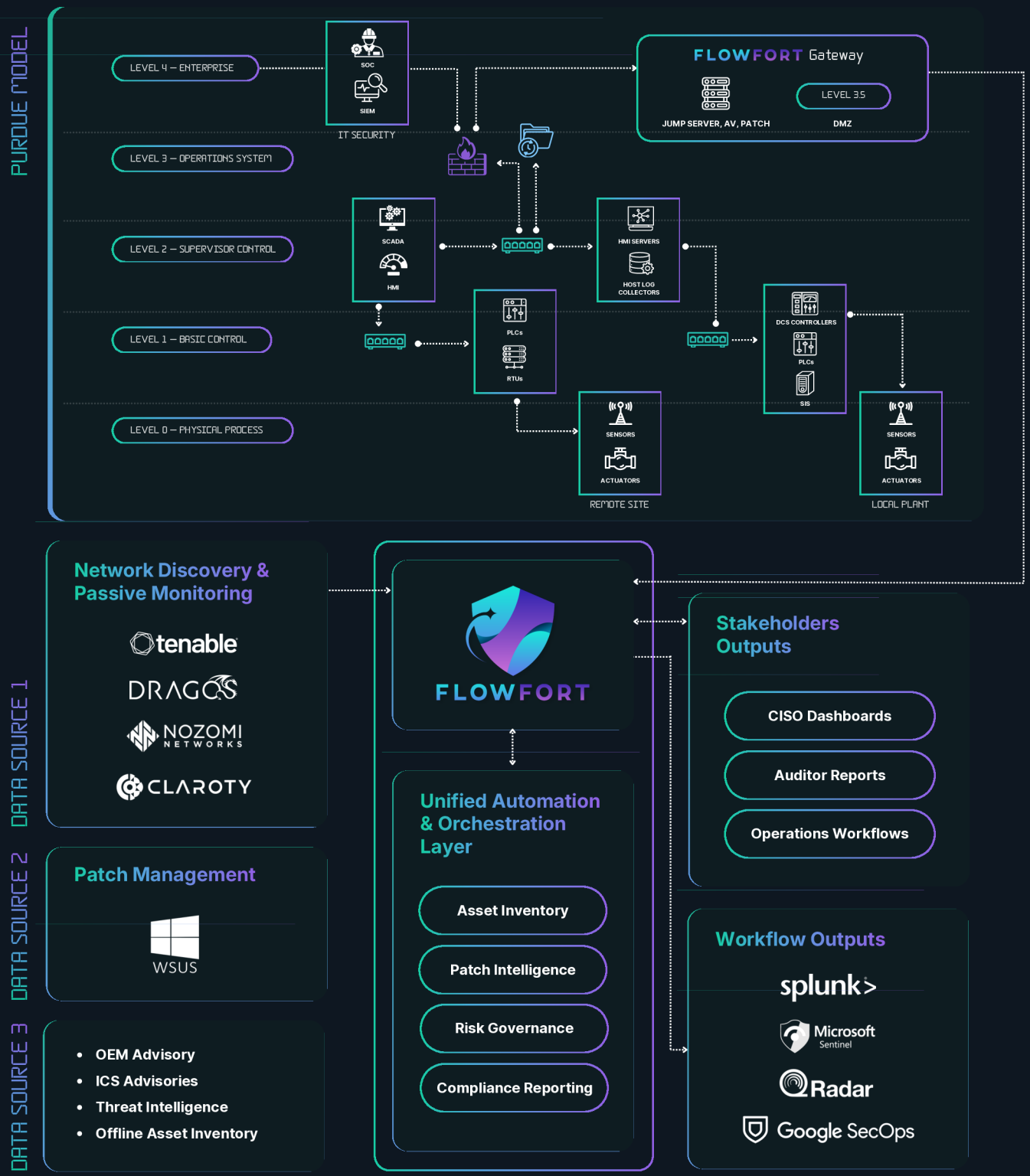
Consider how organizations manage OT security today: detection data lives in one platform, patch data in WSUS or SCCM, risk registers in spreadsheets, maintenance schedules in CMMS or email, compliance evidence on shared drives, and physical asset locations in someone's head, or nowhere. Some detection vendors have begun adding governance-adjacent features: exposure management dashboards, policy compliance checks, or risk scoring overlays. These are valuable incremental steps. But they remain extensions of detection platforms, not purpose-built governance systems with structured workflows, multi-step approval chains, OEM qualification tracking, physical location hierarchies, maintenance window coordination, and audit-ready evidence generation. **The gap is not that no vendor has attempted governance — it is that no vendor has built governance as the primary architecture.** This is what FlowFort was designed to deliver.

Market signals confirm the direction

Multiple signals confirm this direction. Large-scale M&A is targeting the integration of security, risk, and OT into unified operational layers, while Gartner predicts nearly half of CPS buyers will prioritize remediation by 2027. Detection vendors are also shifting toward governance messaging. CISA's August 2025 guidance emphasizes that OT asset inventory delivers real value only when integrated into daily operations, not treated as a one-time project. The market is clearly converging on the governance layer, which FlowFort is built to address.

The OT Cyber Operations Control Plane

FlowFort System Architecture



Progressive Adoption: Start where you are

FlowFort is designed around the same principles used to manage industrial safety and reliability risk — bringing structure, ownership, and repeatability to cybersecurity decisions. Rather than competing with detection platforms, FlowFort absorbs and contextualizes their outputs, combining them with operational, physical, and governance data to form a single decision layer.

FlowFort Convergence Diagram

01

Absorb Detection Context

Ingest asset and vulnerability data from Tenable, Claroty, Nozomi, and others via gateway connectors. Normalize into a unified inventory.

02

Enrich with Operational Context

Map assets to physical locations, maintenance windows, ownership, criticality, dependencies, and lifecycle status across the Purdue model hierarchy.

03

Enable Governed Decisions

Evaluate risks through structured workflows. Assign ownership. Select treatment — Mitigate, Accept, Transfer, or Avoid — with full audit trails and multi-step approval layers.

04

Document for Compliance

Capture evidence automatically. Map decisions to IEC 62443, NIST CSF 2.0, NIS2, Act 854, and sector mandates. Maintain a living compliance posture.

Progressive Adoption: Start where you are

FlowFort does not require organizations to implement every capability on day one. The platform supports progressive adoption aligned to operational maturity:

TIER 1 — *Detection overlay*

Connect FlowFort to existing detection tools (Tenable, Claroty, Nozomi) and WSUS via gateway connectors. Gain a unified asset inventory with vulnerability context and patch status across all sites, replacing fragmented spreadsheets with a single system of record. This tier requires no manual data entry beyond initial gateway configuration.

TIER 2 — *Operational context*

Add asset ownership, criticality scoring, upstream/downstream dependencies, and maintenance window scheduling. Activate risk management workflows and patch approval chains. This tier transforms the platform from an inventory into a governed decision system.

TIER 3 — *Full operational model*

Add physical location modeling with floor plans, IEC 62443 zone and conduit designations, rack diagrams, and full compliance reporting. This tier delivers the complete OT Cyber Operations Control Plane, from detection context through physical reality to audit-ready evidence.

Organizations with limited security staff, including SMEs that make up 97% of Malaysia's manufacturing base, can start at Tier 1 and scale as they mature. MSSPs can handle Tiers 1–2 remotely, adding Tier 3 through periodic on-site support. The platform meets organizations where they are, not where vendors expect them to be.

Operationalizing Industrial Cyber Risk

Industrial cyber risk carries consequences that are physical, operational, and potentially catastrophic — process safety incidents, environmental releases, production shutdowns. Most OT security platforms focus on identifying threats and cataloguing vulnerabilities. **FlowFort focuses on the full risk lifecycle, *especially consequence assessment, risk ownership, and treatment governance.***

STRUCTURED RISK IDENTIFICATION

Configurable forms capture risk title, description, threat scenario, impacted components, and evidence, linking each risk to specific assets or KB articles. Built with FlowFort's visual form builder, sections, question types, and required fields are fully configurable without code.

EDITABLE 5×5 RISK MATRIX

A fully configurable Likelihood × Impact matrix with editable axis labels, numeric scores, and color-coded ratings from Low through Extreme. Both scoring values and rating labels are editable — calibrated to your organization's risk appetite, not a static template.

FORMAL TREATMENT STRATEGIES

Four treatment options; Avoid, Accept, Transfer, Mitigate. Each with strategy-specific fields. Avoidance requires a defined action and timeline. Acceptance requires documented justification and a named owner. There is no path to undocumented risk acceptance.

MULTI-STEP APPROVAL WORKFLOWS

Configurable approval layers route risks through designated reviewers and approvers. Review cycles; quarterly, bi-annually, or annually, are enforced by the platform, not left to calendar reminders. Pending and decided states maintain full audit history.

MITIGATION ACTION TRACKING

A kanban-style view tracks all actions linked to parent risks. Each action has an owner, target date, status, and evidence trail. Executive dashboards surface total risks, high residual risk count, overdue reviews, and longest-open risks with named owners.

OT-Aware Patch Qualification & Governance

In IT, patches deploy automatically across thousands of endpoints within hours. In OT, a single unqualified patch can crash a safety controller, halt a production line, or cause a hazardous process failure. This is why 85% of organizations don't patch regularly. The barriers are structural: devices must be taken offline, OEM qualification is required, maintenance windows are scarce, and vendor diversity makes centralized management nearly impossible.

FlowFort doesn't simply push patches. It provides the ***intelligence, qualification, and governance layer*** that makes OT patching feasible, safe, and auditable.

IEC 62443 RECOGNIZES WSUS — BUT WSUS ALONE IS NOT ENOUGH

IEC 62443-2-3 explicitly recognizes WSUS as an approved mechanism for distributing patches to Windows-based OT assets. Many organizations already have WSUS deployed in their OT networks. However, WSUS is a distribution tool, **not a governance platform**. It lacks multi-layer approval workflows, OEM qualification tracking, risk-based prioritization, maintenance window coordination, and audit-ready documentation. A patch approved in WSUS is a patch pushed to a device, with no stage gate for OEM verification, no formal sign-off from operations, and no documented risk assessment if deferred. **FlowFort** integrates directly with WSUS to leverage its distribution capability while adding the governance layers that IEC 62443 demands.

01

Patch Inventory & Scoring

Track all KB articles with configurable patch priority scores, OEM qualification status, and qualified dates. Color-coded scoring enables instant triage.

02

OEM Qualification Tracking

Knowledge Base Verification captures vendor, product, version, OS compatibility, and evidence — reference URLs, portal links, email proof, for every qualified patch.

03

Request & Approval Workflow

Deploy by asset or by KB article. Multi-step approval routes through designated approvers. Full audit trail from request to deployment.

04

Installation Tracking

Monitor per-device deployment status. Track success, failure, and pending states with linked site and device context.

FLOWFORT PATCH PRIORITY SCORE

$$\text{Score} = (TI \times 0.20) + (BI \times 0.15) + (PI \times 0.20) + (PL \times 0.25) + (EX \times 0.20)$$

Each factor is scored on a 1-5 scale

TI = Threat Intel (5 = Actively Exploited / Zero-Day, 4 = High, 3 = Medium, 2 = Low, 1 = No Known Exploit)
BI = Business Impact • PI = Process Impact • PL = Patch Level • EX = Exposure

All factors use the same 1-5 scale; all weightages are fully configurable to match your organization's risk appetite. Scores are assigned per-asset by the platform based on integrated data sources (Tenable, WSUS) and enriched by site operators who understand local process context.

Location Aware Asset Modeling

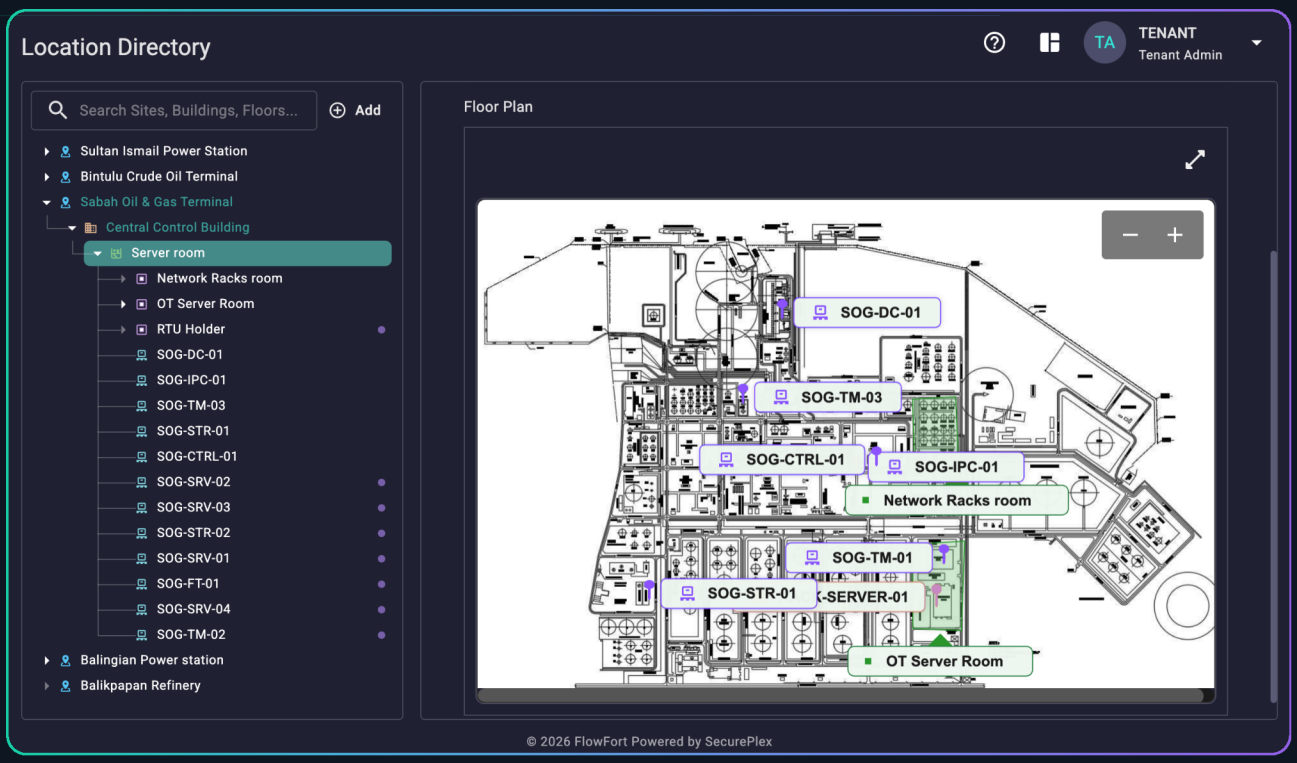
The first rule of OT security is well understood: **You cannot protect what you don't know**. But field practitioners have discovered an equally important second rule: **You cannot act on what you cannot physically locate.**

OT cybersecurity consultants working across Southeast Asian industrial sites consistently report the same challenges: extended project scoping due to inaccurate inventories, inability to determine physical asset locations despite automated discovery, discrepancies between inventories and risk assessments, and incomplete asset data preventing vulnerability identification.

CISA's landmark August 2025 guidance — "Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators," co-authored with NSA, FBI, EPA, and five international partners, outlines a five-step lifecycle: define scope, identify assets, create taxonomy, manage data, and implement lifecycle management. Critically, CISA emphasizes that the real value comes when the inventory is integrated into daily operations — enabling prioritization by criticality, detection of unauthorized devices, network segmentation, and rapid incident response. CISA references ISA/IEC 62443 as the foundation for OT taxonomies using zones and conduits.

FlowFort

Floor Plan Editor



FlowFort implements every CISA recommendation as platform capability:

- Hierarchical location mapping with CAD-style floor plan editing
- IEC 62443 zone and conduit designations per space
- Geospatial site context with embedded maps
- Asset-to-location binding with rack diagrams
- Dependency maps showing upstream/downstream relationships with process impact ratings

This is the **bridge between cybersecurity data and operational reality** that **detection platforms cannot provide.**

Four Scenarios That Change How You Respond

Detection tools generate alerts. Without operational context, ***every alert looks the same.*** **FlowFort transforms alerts from ambiguous signals into informed decisions** by enriching them with physical, operational, and ownership context.

SCENARIO 1 : THE FALSE POSITIVE THAT WASTES 48 HOURS

Without FlowFort

Your detection platform flags repeated failed login attempts on a DCS controller at 2:00 AM. The SOC classifies it as a brute-force attack. An IR team is mobilized. After 48 hours of investigation, the team discovers a maintenance engineer was performing a scheduled firmware upgrade and had forgotten the controller's credentials after a recent password rotation.

With FlowFort

The analyst cross-references the asset and immediately sees: the asset is under an approved maintenance window (1:00–5:00 AM), linked to a firmware upgrade, with the assigned engineer listed as maintainer. The alert is closed as known operational activity within minutes.

SCENARIO 2 : THE REAL INCIDENT WHERE YOU CAN'T FIND THE ASSET

Without FlowFort

Anomalous Modbus traffic from a controller — possible command injection. Where is this device? Who owns it? What depends on it? The security team has an IP address. The OT engineering lead is on leave. The site manager thinks it's in Building 3 — or Building 5. Response is delayed hours while the team manually traces connections and walks the plant floor.

With FlowFort

The analyst searches the asset and instantly sees: Central Control Building, Server Room, Zone 1, Rack 3. The asset owner is listed. The dependency map shows two upstream sensors and one downstream HMI. The process impact rating is "High." The analyst has everything needed for an informed isolation decision in minutes, documented in the platform.

SCENARIO 3 : THE VULNERABILITY THAT'S ALREADY MITIGATED

Without FlowFort

A critical CVE affects three PLCs. The security team treats all three as equally urgent, potentially disrupting operations for emergency patching. They don't know that two are behind segmentation blocking the exploit vector, and the third has a firmware update already queued in next week's maintenance window.

With FlowFort

The vulnerability dashboard shows all three assets with zone designations, current patch status, and linked maintenance plans. Two have documented compensating controls; the third has an approved patch request with OEM qualification complete. The response is a status update, not an emergency — and the audit trail proves the risk was already managed.

SCENARIO 4 : THE CASCADING FAILURE NOBODY PREDICTED

Without FlowFort

Ransomware encrypts a historian server. The response focuses on that server. But nobody realized it was the upstream data source for three HMI displays. When the historian goes down, operators lose visibility into tank levels and pressure readings, triggering an emergency shutdown. The cascade was invisible because dependencies were never documented.

With FlowFort

The dependency map surfaces all downstream assets before isolation. The IR team coordinates with operations to switch to manual monitoring for specific process variables, preventing the cascade. The dependency data exists because FlowFort requires it during asset onboarding.

Built for Distributed Industrial Operations

Industrial organizations operate across geographically distributed sites spanning multiple countries and regulatory jurisdictions, with different connectivity profiles and operational teams. **FlowFort** is **built as a multi-tenant SaaS platform with a hybrid architecture** that ***balances centralized governance with distributed execution.***

GATEWAY ARCHITECTURE

Secure gateway connectors at each site bridge the gap between OT networks and FlowFort. Gateways sync asset and vulnerability data from Tenable and WSUS without exposing OT networks to the internet. Sites with intermittent connectivity continue to operate autonomously.

ROLE-BASED ACCESS CONTROL

Nine system-defined roles, from Tenant Admin (full access) to Site Operator (limited, site-scoped), plus custom user-defined roles. Enterprise SSO integration with Azure AD, Google, and Okta.

CONFIGURABLE APPROVAL WORKFLOWS

Four workflow types; Maintenance Approvers, Site Maintenance, Risk Management, Patch Installation, each with multi-step routing. No patch is deployed, no risk is accepted, and no maintenance window is opened without the appropriate authorization chain.

MAINTENANCE SCHEDULING WITH BUSINESS LIMITS

Your detection platform flags repeated failed login attempts on a DCS controller at 2:00 AM. The SOC classifies it as a brute-force attack. An IR team is mobilized. After 48 hours of investigation, the team discovers a maintenance engineer was performing a scheduled firmware upgrade and had forgotten the controller's credentials after a recent password rotation.

MSSP AND CHANNEL PARTNER ENABLEMENT

FlowFort's multi-tenant architecture is designed for managed security service providers (MSSPs) and system integrators serving the OT security market. Each customer operates in an isolated tenant with dedicated configuration, while the MSSP maintains centralized visibility across their portfolio. This model is critical in Southeast Asia, where the cybersecurity talent shortage, an estimated 2.8 million unfilled roles across ASEAN which means that most industrial organizations will rely on managed services for OT security. FlowFort gives MSSPs the operational platform to deliver patch management, risk governance, and compliance reporting as a managed service, capabilities that detection-only platforms cannot support.

SOUTHEAST ASIA: THE RIGHT PLATFORM FOR THE REGION'S REALITY

Southeast Asia's industrial cybersecurity landscape presents a unique combination of rapid regulatory maturation (Malaysia's Act 854, Singapore's OT Masterplan), massive industrial footprints (national oil companies, state utilities, multinational refining and mining operations), and severe capability gaps (97% of Malaysia's manufacturing base is SME). The region needs platforms that can scale from a single palm oil mill to a multi-country refinery group, delivering enterprise-grade governance without requiring enterprise-grade security teams. FlowFort's multi-site management, configurable workflows, and ASEAN-relevant compliance mapping (Act 854, Singapore CII requirements) are purpose-built for this market.

The Commercial Case For Post-Discovery Governance

Investments in OT security are typically justified through risk reduction. But post-discovery governance delivers measurable operational returns that extend beyond cybersecurity:

01 *Reduced Incident Response Time*

The operational scenarios in this whitepaper illustrate the difference: a false-positive investigation that takes 48 hours without context takes minutes with FlowFort's maintenance window awareness and asset ownership data. At typical manufacturing downtime costs of $50,000–$125,000 per hour, even a single avoided false-positive shutdown pays for the platform.

02 *Compliance Cost Reduction*

Audit preparation in most OT environments is a weeks-long scramble to assemble evidence from disparate systems. FlowFort generates compliance evidence as a byproduct of normal operations — vulnerability assessments, patch management summaries, and risk assessment reports — on-demand or automatically scheduled. Organizations that have implemented structured compliance platforms report reducing audit preparation from weeks to days.

03 *Patch Cycle Acceleration*

With an average of 69 days to apply OT patches, every day saved in the qualification and approval process reduces the window of exposure. FlowFort's OEM qualification tracking, integrated approval workflows, and maintenance scheduling coordination compress the time from vulnerability discovery to safe deployment — without bypassing the governance steps that prevent operational disruption.

04 *Reduced Risk Of Regulatory Penalty*

NIS2 penalties reach €10 million or 2% of global revenue. Malaysia's Act 854 carries RM 500,000 fines and 10 years imprisonment. The cost of non-compliance now significantly exceeds the cost of governance tooling — and the gap is widening with every regulatory update.

THE TOTAL COST OF FRAGMENTATION

Consider the hidden costs of the current approach; Detection platform licenses (typically $15–40 per asset per year), plus manual patch tracking in spreadsheets (FTE time), plus risk registers in Excel (audit prep time), plus compliance evidence assembly (weeks of FTE effort per audit), plus incident response delays (hours of production downtime per false positive), plus regulatory penalty exposure. FlowFort consolidates the governance layer into a single platform, reducing operational overhead, accelerating response, and providing audit-ready documentation as a natural byproduct of the workflow.

FLOWFORT

A UNIFIED OT PATCH, RISK & COMPLIANCE MANAGEMENT

To learn more about how Flowfort can support your organization,

CONTACT US TO LEARN MORE

hello@secure-plex.com

+603-2242 4363

Level 6, Menara TH, Tower 2A, Avenue 5, The Horizon, Bangsar South, 59200, Kuala Lumpur.