SecFlowX

Product Sheet

PeakCyber

OVERVIEW

What Is SecFlowX

SecFlowX is a Security Posture Management (SPM) platform developed by PeakCyber. It unifies asset discovery, vulnerability management, scan orchestration, workflow automation, and compliance reporting into a single cohesive platform.

Rather than replacing existing security tools, SecFlowX orchestrates them, aggregating their findings, normalizing their data, and providing the automation and reporting layer that transforms raw scanner output into actionable security intelligence.

Security, development, and IT operations teams share a single source of truth, enabling faster detection-to-remediation cycles at enterprise scale.

At a Glance

68+ Active integrations

10+ Integration categories

6 Asset types supported

1 Unified platform

KEY CAPABILITIES

What SecFlowX Does

Unified Asset Inventory
Continuously tracks source code repos, domains, ip's, container images, kubernetes clusters, and cloud resources. Multi-source ingestion from VCS, CMDB, EDR, and scanner platforms.

Centralized Vulnerability Management
Single pane of glass for all scanner findings with CVSS v3.1 scoring, full lifecycle tracking, bulk triage, and deduplication across tools.

Scan Orchestration
Trigger and manage SAST, DAST, SCA, secret, and infrastructure scans from a single control plane. Normalized output across all tools.

Supply Chain Security (SBOM)
CycloneDX/SPDX bill of materials with component-level CVE correlation, quality scoring, and automatic CI/CD pipeline generation.

Workflow Automation
No-code visual workflow builder with triggers, conditional rules, and actions — auto-create Jira tickets, send Slack/Teams alerts, assign owners.

Issue Management
Bidirectional Jira synchronization (Cloud & On-Premise), Kanban board, dynamic templates, and full activity timelines.

Misconfigurations
Ingests Prowler and cloud findings with CIS Benchmark mappings, pass/fail history, and step-by-step remediation guidance.

Approvals & Governance
Structured approval workflows for risk exceptions and false positives — with mandatory expiry dates and a full auditable decision trail.

AI-Powered Remediation Guidance
Context-aware fix recommendations via OpenAI, Gemini, and other LLM integrations to accelerate mean time to remediation.

Reports & Analytics
One-click professional PDF reports from live data. Configurable templates, CDN storage, and full historical retention for audit reviews.

BUSINESS OUTCOMES

Why It Matters

Hours → Seconds
Detection-to-assignment for critical findings

Zero blind spots
Full asset coverage including shadow assets

100% auditable
Every exception, approval & action logged

1-click reports
Compliance-ready PDFs from live platform data

Proactive, Not Reactive
SLA-driven remediation tracking surfaces overdue items automatically before they become incidents.

Integrated with Dev Workflows
CI/CD pipeline gates block releases with unresolved Critical or High findings — security enforced at the source.

Measurable Risk Posture
Unified risk dashboard consolidates all integration data into a real-time executive view, measurable over time.

INTEGRATION ECOSYSTEM

68+ Integrations — Orchestrate Your Existing Toolchain

SecFlowX connects to your current security investments across 10+ categories. No rip-and-replace — pure orchestration. Each integration supports multiple simultaneous instances. Missing a tool? Let us know, we will integrate for you.

SAST SonarQube · Semgrep · Checkmarx · Snyk Code · Fortify · Bandit · Gosec · Checkov · Aikido	**DAST** OWASP ZAP · Nuclei · MobSF	**SCA** Dependency-Track · Grype · Trivy · Prisma Cloud · GitHub Dependabot · XEOL · Dependency Check
Secret Scanning TruffleHog · GitLeaks · GitHub Secret Scanning	**Infrastructure** Prowler · AWS Inspector · Tenable · RoxCTL · CrowdStrike	**Version Control** GitHub · GitLab · Bitbucket Cloud & On-Premise
Task Management Jira Cloud · Jira On-Premise/DC · SecFlowX Native	**Notifications** Slack · Microsoft Teams · SMTP Email	**AI** OpenAI · Gemini · Other LLM providers
Authentication LDAP · SSO	**Training** Secure Code Warrior	**Cloud Platforms** AWS · Microsoft Azure · Google Cloud Platform

TECHNICAL HIGHLIGHTS

Built for Enterprise Scale

On-Prem & Multi-Tenant
Modern architecture with full organizational isolation, API-first design, and configurable role-based access control.

CLI & REST API
All platform functionality exposed via REST API and a DevSecOps-ready CLI — integrate with any CI/CD platform.

RBAC & Audit Logging
Granular permissions with immutable audit logs capturing every action — who, what, when, and via which endpoint.

SLA Management
Severity-based SLA policies with automated escalation, team performance measurement, and overdue reporting.

USE CASES

SecFlowX in Action

01 **Centralizing a Multi-Scanner Security Program**

A financial services organization runs SonarQube, OWASP ZAP, Dependency-Track, Prowler, Tenable, and TruffleHog. SecFlowX connects all six, normalizes output, and delivers a single security posture dashboard — eliminating hours of weekly manual aggregation.

02 **Automated Critical Vulnerability Response**

Workflow triggers on CVSS ≥ 9.0 linked to a production asset — automatically creates a Jira ticket, assigns it to the on-call lead, and fires a Slack alert. Mean time from detection to assignment drops from hours to seconds.

03 **Release Gate Security Validation**

The SecFlowX CLI is invoked from every CI/CD run. It queries for open Critical/High findings on the release artifact and returns a non-zero exit code to block deployment until findings are remediated or formally accepted.

04 **Zero-Day Blast Radius Assessment**

When a critical CVE is disclosed, the security team queries SecFlowX across all asset types by CVE ID. Assets are grouped by team and criticality — reducing multi-day cross-tool investigations to a single query with actionable output.

See SecFlowX in Action

Request a product demonstration, technical evaluation, or integration deep-dive.

Contact via secflowx.com