SPARROW

# Sparrow Enterprise

## AI-Powered Integrated Application Security Testing

ISO 26262

By consolidating application security testing solutions into a single system, organizations can reduce software development time and costs, while enabling the systematic and effective implementation of DevSecOps.

Integrated Application Security for
Proactive Software Supply Chain Security

# Sparrow Enterprise

**Sparrow Enterprise** delivers an AI-powered unified environment for analyzing source code (SAST), open-source components (SCA), and running applications (DAST). By shifting security left, the platform identifies risks early in the SDLC, ensuring the delivery of secure, resilient software while minimizing costly rework. Furthermore, its SBOM-based license and vulnerability management capabilities enhance protection against critical software supply chain threats.

## Main Features

Sparrow Enterprise provides comprehensive vulnerability analysis throughout the Software Development Life Cycle, backed by advanced analysis and management capabilities to enhance an organization's overall security posture.

| Dashboard | Issue Tracking by Asset<br>(SAST, DAST, & SCA Issues) | Asset Overview<br>(Total & Risky Assets, Components) | Issue Status<br>(By Risk Level, Status, Time) | Approval Status<br>(Ongoing & Pending Approvals) |
|---|---|---|---|---|

| Analysis Features | Source Code Analysis | Component Analysis | Web Vulnerability Analysis | Analysis Automation |
|---|---|---|---|---|
| | Security Vulnerability Analysis<br>Code Quality (Defect) Analysis<br>Identify Exact Locations of Issues<br>Secure Code Examples / Recommended Fixes | Component Identification<br>Verify License Disclosure/ Obligations<br>Detect and Validate Vulnerabilities<br>Generate and Export SBOM (Software Bill of Materials) | Select Analysis Target (URL, OpenAPI)<br>Configure Analysis Scope (URL Crawl Depth, Excluded URLs, etc.)<br>Reproduce / Simulate Attack Sequences | Integrations with Heterogeneous Tools (Version Control Systems, CI/CD Tools, etc.)<br>Real-Time Monitoring of Analysis Status (Running, Paused/Stopped, Completed) |

| Management Features | User | Approval | Issue Status | Rule and Work Profile | Report |
|---|---|---|---|---|---|
| | User & User Group<br>Role and Permission<br>View Analysis / Audit History | Configure Approval Lines<br>Set Approval Scope (Project, System)<br>Manage Approval Targets (Issues, Assets, Components, etc.) | Assign Reviewers<br>Change Issue Status (To do, Doing, Done) | Choose Policy-Based Detection Rules (OWASP Top 10, CWE, etc.)<br>Classify Issues into 5 Risk Levels (Critical, High, Medium, Low, Trivial)<br>Customizable Rule and Option | Customizable Report Template (Title, Logo, etc.)<br>Configure Report by Reference (OWASP, CWE, etc.)<br>Customizable Items (Risk Level, Rule, Asset, etc.) |

| AI Features | Open Source AI Model Usage Check | AI-Powered Remediation Suggestion | Intelligent Prioritization |
|---|---|---|---|

# Analysis Technology

Sparrow Enterprise strengthens software supply chain security by providing comprehensive analysis of source code, open-source, and web vulnerabilities across the entire SDLC and operations.

### Source Code Analysis
### SAST/SAQT

**Secure Coding with Source Code Analysis:** Detects latent security vulnerabilities and code quality defects directly within the source code.

- Supports analysis of 25+ languages (including C/C++, Java, Python, etc.), frameworks, and Infrastructure as Code (IaC)
- Identifies exact locations and root causes of vulnerabilities based on actual source code
- Provides secure code examples to guide remediation of findings

### Component Analysis
### SCA

**Software Bill of Materials (SBOM) & Open Source Governance:** Identifies open-source components, retrieves license and vulnerability information, and automatically generates a Software Bill of Materials (SBOM).

- SBOM Generation & Management: Generates comprehensive Software Bill of Materials (SBOM) in industry-standard formats like SPDX and CycloneDX
- Automatically identifies open-source licenses, including open-source AI models, and provides notification obligations
- License Compliance: Real-time monitoring of open-source licenses to prevent legal risks and ensure intellectual property protection

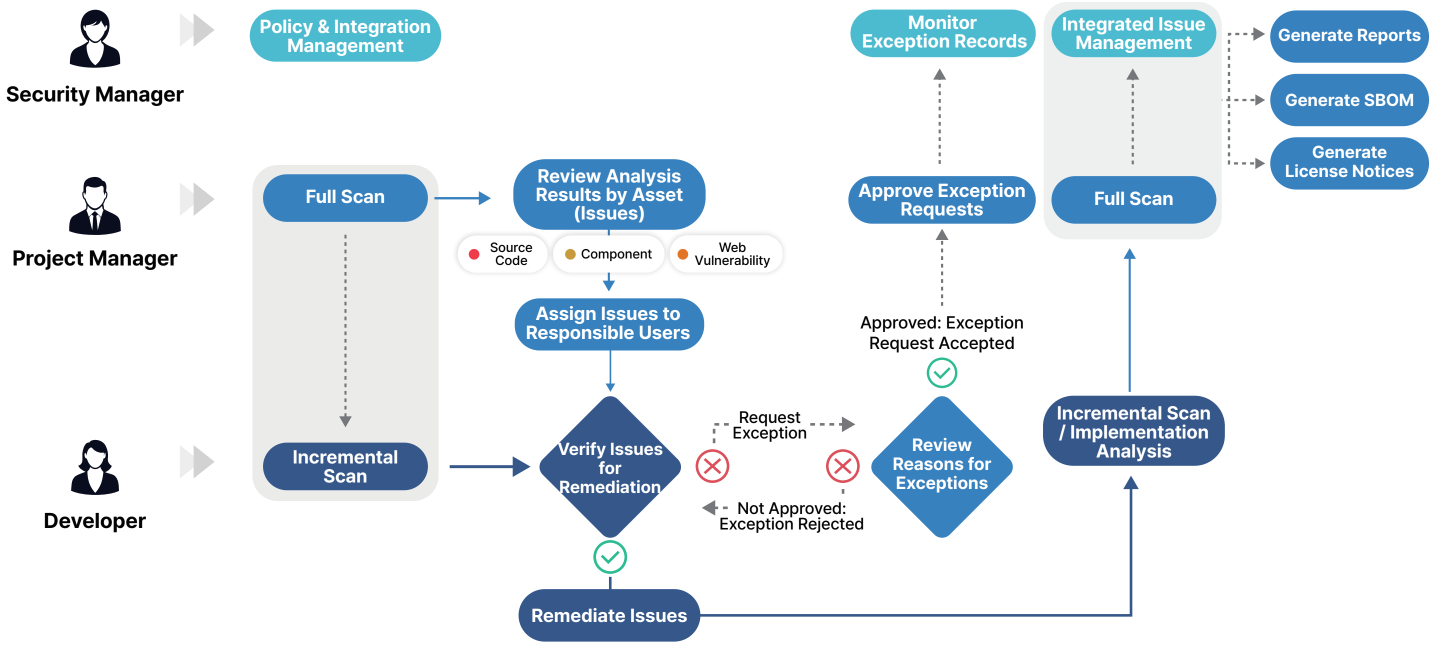
### Web Vulnerability Analysis
### DAST

**Web Vulnerability Detection:** Detects runtime vulnerabilities in web applications that static analysis can miss by testing the application during execution.

- Performs analysis from a site's root URL or based on an OpenAPI specification
- Fine-tunes crawl/scan options (URL crawl depth, excluded URLs, SSL certificate usage, etc.)
- Provides explanations of discovered vulnerabilities along with remediation guidance
- Supports API security analysis based on the OWASP API Top 10

# Analysis & Issue Management Process

Centralized Policy, Role, and Scan Management: Establish consistent security policies across the entire SDLC, assign differentiated user roles and permissions, and perform regular full and incremental scans. Manage results by asset and by issue for effective threat response.



Security Manager

Policy & Integration Management

Monitor Exception Records

Integrated Issue Management

Generate Reports

Generate SBOM

Generate License Notices

Project Manager

Full Scan

Review Analysis Results by Asset (Issues)

● Source Code ● Component ● Web Vulnerability

Assign Issues to Responsible Users

Approve Exception Requests

Full Scan

Approved: Exception Request Accepted

Developer

Incremental Scan

Verify Issues for Remediation

Request Exception

Not Approved: Exception Rejected

Review Reasons for Exceptions

Incremental Scan / Implementation Analysis

Remediate Issues

| Integration | Internal Systems | DevOps Tools |
|---|---|---|
| | HR Systems, Email/Messaging Platforms, Authentication Solutions, etc. | Version Control Systems, CI/CD Tools, Issue Tracking Systems, etc. |

# Implementation Benefits

Centrally manage application security vulnerabilities within a single, AI-powered platform to proactively address threats throughout the SDLC. By establishing a systematic remediation process, organizations can minimize resource waste and effectively strengthen their software supply chain security.

## 1 Minimize Security Blind Spots with an Integrated Solution

- Sparrow Enterprise integrates SAST, SCA, and DAST into a single environment to detect complex vulnerabilities that siloed tools often miss
- By performing integrated analysis across various applications, the platform provides comprehensive coverage and minimizes security blind spots
- Consistent security policies are applied throughout the software development lifecycle to ensure high-visibility risk management

## 2 Achieve DevSecOps with AI-Driven Proactive Remediation

- Automate security testing at every stage by integrating directly into your DevOps pipeline
- Enables development and security teams to respond to threats using the same standards, maintaining an ideal balance between development speed and security
- Identifying and fixing vulnerabilities early in the development process prevents costly rework and realizes a true DevSecOps workflow

## 3 Maximize Operational Efficiency with Intelligent Prioritization

- Gain immediate visibility into asset security and remediation status through a unified, centralized management dashboard
- AI-powered prioritization and vulnerability reproduction features allow teams to focus on the most critical issues first, significantly reducing response times
- A customizable approval process and integrated issue tracking eliminate duplicate work and enhance collaboration between cross-functional teams

# Customers

With outstanding analysis capabilities and user-friendly convenience, Sparrow solutions are trusted by public institutions and enterprises to ensure the security of their software supply chains.

| | |
|---|---|
| **Government & Public Sector** | Ministry of Justice, Ministry of Employment and Labor, Ministry of Foreign Affairs, Ministry of Trade, Industry and Energy, Supreme Court of Korea, Public Procurement Service, Korea Meteorological Administration, Ministry of Data and Statistics, Korean Intellectual Property Office, National Tax Service, Korea Customs Service, National Police Agency, National Assembly Secretariat, Korea Internet & Security Agency (KISA), Incheon International Airport Corporation, Korea Airports Corporation, Korea Asset Management Corporation, Korea Deposit Insurance Corporation, KEPCO Engineering & Construction Company, Inc., Korea Gas Corporation, Korea Water Resources Corporation, Korea Public Finance Information Service, Korea Credit Information Services, Korea Housing Finance Corporation, Korea Housing & Urban Guarantee Corporation, Korean Broadcasting System (KBS) |
| **Financial Sector** | Financial Supervisory Service, Korea Financial Telecommunications & Clearings Institute, Bank of Korea, KB Kookmin Bank, Shinhan Bank, NongHyup Bank, Korea Development Bank, IM Bank, Korea Investment & Securities, KakaoPay Securities, Kyobo Securities, Kiwoom Securities, KB Kookmin Card, Woori Card, Lotte Card, NongHyup Card, NH NongHyup Property & Casualty Insurance, AXA General Insurance, Lotte Insurance, Korean Reinsurance Company, Samsung Life Insurance, NH NongHyup Life Insurance, Hana Life, KB Capital, Meritz Capital, Danal, Finnq, Koscom, NICE Information Service, SBI Savings Bank, Korea Investment Savings Bank, IBK Savings Bank, MG Community Credit Cooperatives |
| **Enterprise & Industry** | Samsung SDS, Naver Cloud, CJ OliveNetworks, KT, Kakao Enterprise, NHN, Lotte Innovate, NCSOFT, Neople, Hyundai Motor Company, GS Caltex, POSCO, SK Chemicals, Hyundai Rotem, Hanwha Aerospace, SEMES, 42dot, Hanwha Ocean, HMM, STX Engine, CJ Logistics, TMAP Mobility, GS Retail, Homeplus, Dongkuk Steel |
| **Defense & Security** | Republic of Korea Army, Navy, Air Force, Defense Acquisition Program Administration, Military Manpower Administration, Cyber Operations Command, Defense Communication Command, Korea Institute for Defense Analyses, Defense Agency for Technology and Quality, National Security Research Institute, LIG Nex1, Hanwha Systems |
| **Global** | Public Sector (Malaysia), Financial Sector (Japan), Manufacturing (Japan, China), Healthcare (Japan), R&D (Japan, China), IT (Japan, China), Security (Singapore), and Partners in Japan, China, India, Malaysia, Vietnam, Indonesia, and the United Arab Emirates |

For more information,

## Contact Sparrow Team Now!

✉ E. marketing@sparrow.im

🎧 T. +82-2-6263-7400

Sparrow Website

sparrow.im