INVICTI ASPM

APPLICATION SECURITY POSTURE MANAGEMENT

eVolcano Inc.
Authorized Partner

수천 개의 경고 알림 속에서
진짜 위험을 찾아내는
유일한 통찰력.

도구는 많아졌지만, 보안은 더 복잡해졌습니다.
흩어진 보안 데이터를 통합하고, 비즈니스 맥락에 맞춰 진짜 고쳐야 할 취약점만 선별하는 ASPM(애플리케이션 보안 태세 관리)을 만나보십시오.

UNIFIED VISIBILITY

통합 가시성 확보

DAST, SAST, SCA, Cloud 등 파편화된 보안 도구의 데이터를 한 곳에 모아 전체 애플리케이션 보안 상태를 조망합니다.

DATA CORRELATION

데이터 상관분석 및 중복 제거

서로 다른 도구에서 발견된 동일한 취약점을 매핑하고 중복을 제거(De-duplication)하여, 개발자가 처리해야 할 '노이즈'를 줄입니다.

RISK-BASED

비즈니스 기반 우선순위 식별

단순 심각도가 아닌, 자산의 중요도와 실제 악용 가능성(Exploitability)을 반영한 '진짜 위험' 순서대로 조치하도록 가이드합니다.

THE NEW STANDARD

왜 지금 ASPM(보안 태세 관리)인가?

기업당 평균 50~100개의 보안 도구를 사용하지만, 가시성은 오히려 떨어지고 있습니다.
"Tool Sprawl(도구 난립)" 문제를 해결하고 보안 데이터를 하나의 맥락으로 연결해야 합니다.

KEY DRIVER

"취약점의 수(Volume)보다 해결 시간(Velocity)과 위험(Risk)에 집중해야 한다."

현대적인 AppSec 프로그램의 핵심 전환점

Consolidate
Siloed Data

Invicti ASPM의 6단계 핵심 수명주기

1 자산 식별 (Discover)
Asset Inventory

클라우드, 온프레미스, 코드 저장소, API 등 조직 내 모든 애플리케이션 자산을 자동으로 찾아내어 카탈로그화합니다.

2 데이터 수집 (Ingest)
Integration

SAST, DAST, SCA, Container Scan 등 다양한 써드파티 보안 도구의 결과 데이터를 Invicti ASPM으로 통합 수집합니다.

3 상관 분석 (Correlate)
De-duplication

동일한 취약점을 가리키는 서로 다른 도구의 결과를 하나로 매핑하고 중복을 제거하여 관리 포인트를 획기적으로 줄입니다.

4 우선순위화 (Prioritize)
Risk Scoring

자산의 중요도(Business Criticality)와 악용 가능성(EPSS 등)을 결합하여, 당장 고쳐야 할 상위 1%의 위험을 선별합니다.

5 조치 및 추적 (Remediate)
Workflow Automation

개발자가 사용하는 Jira, GitLab 등의 툴로 티켓을 자동 할당하고, 수정 여부를 자동으로 다시 확인(Retest)합니다.

6 성과 측정 (Measure)
AppSec KPIs

단순 발견 수가 아닌 MTTR(평균 조치 시간), 스캔 커버리지 등 실질적인 보안 성과 지표를 대시보드로 시각화합니다.

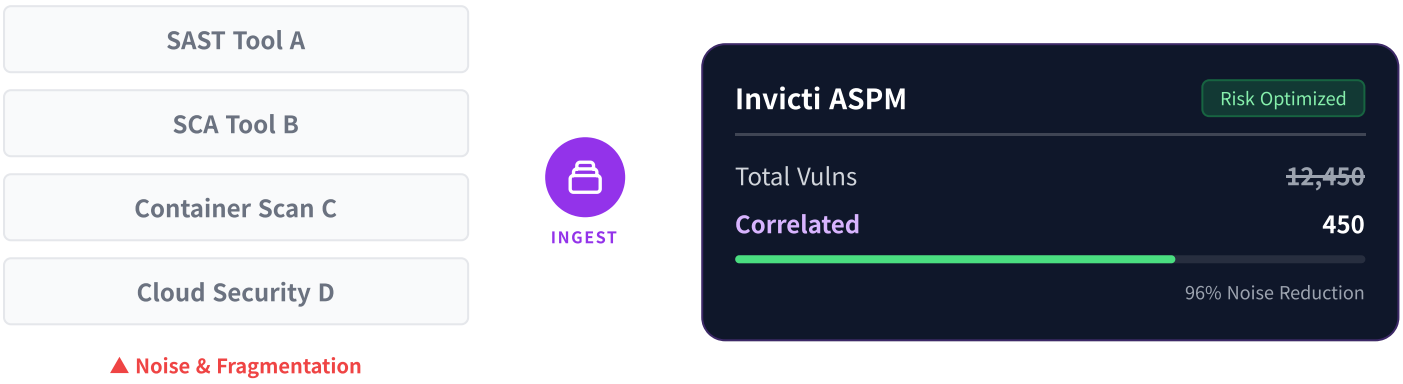
복잡한 AppSec을 하나의 플랫폼에서 통제하는 힘

Invicti ASPM

UNIFIED PLATFORM

파편화된 도구들을 통합 인텔리전스로

개별적으로 동작하는 SAST, SCA, DAST 도구들은 각각 수백 개의 경고를 쏟아냅니다. Invicti ASPM은 이들을 **단일 뷰(Single Pane of Glass)**로 통합하여, 보안 팀이 전체 그림을 보고 전략적 의사결정을 내릴 수 있도록 지원합니다.



How Correlation Works

단순한 리스트 합치기가 아닙니다. Invicti ASPM은 다음과 같은 고유 식별자를 사용하여 데이터를 매핑합니다.

- **File Path & Line Number:** 소스 코드(SAST)와 실행 결과(DAST/IAST) 매칭
- **Endpoint URL:** 웹 애플리케이션 스캔 결과와 API 정의서 매칭
- **CVE ID:** 알려진 취약점 데이터베이스를 통한 공통 식별

Ingestion Sources

업계 표준 포맷(SARIF, JSON 등)을 지원하여 모든 최신 보안 도구를 수용합니다.

- **Code Scanners:** SonarQube, Checkmarx, Fortify
- **Dependency Check:** Snyk, Black Duck, Mend.io
- **Cloud/Container:** AWS Inspector, Trivy, Clair

Integrate with Your Ecosystem

ISSUE TRACKERS	CI/CD	SCANNERS	COMMUNICATION
Jira, Azure DevOps	**Jenkins, GitHub**	**Snyk, SonarQube**	**Slack, MS Teams**
Benefit 티켓 상태 양방향 자동 동기화	**Benefit** 빌드 파이프라인 내 보안 게이팅	**Benefit** 이기종 보안 데이터 통합/정규화	**Benefit** 이슈 발생 시 즉각적인 팀 알림

- **Continuous DAST Verification**

Invicti의 DAST 엔진은 ASPM의 단순 데이터 소스가 아닙니다. 통합된 타사 취약점(SAST 등)을 **동적으로 재검증(Re-validate)**하여 오탐을 제거하는 '검증 엔진' 역할을 수행합니다.

THE PAIN POINT

보안 부채(Security Debt)의 늪

경고 피로 (Noise)

- **False Positives:** 보안 도구의 오탐율은 평균 40% 이상입니다. 개발자는 '진짜 버그'를 찾기 위해 시간을 허비합니다.
- **Context Missing:** 테스트 환경의 취약점과 운영 환경의 치명적 결함이 동일한 'High' 등급으로 표시됩니다.
- **Duplicate Issues:** SAST와 DAST가 동일한 문제를 중복 보고하여 업무량이 2배로 늘어납니다.

가시성 부재 (Blind Spots)

- **Shadow IT:** 개발팀이 보안팀 승인 없이 띄운 클라우드 인스턴스와 API가 방치됩니다.
- **Incomplete Inventory:** 엑셀로 관리되는 자산 목록은 하루만 지나도 낡은 정보가 됩니다.
- **Tool Silos:** 각 도구의 대시보드가 분리되어 있어 전체 보안 태세를 한눈에 파악할 수 없습니다.

THE SOLUTION

ASPM: 진짜 중요한 문제 해결

Focus

맥락 기반 우선순위

- **EPSS Score:** 실제 해커가 악용 중인 취약점인지 점수화
- **Asset Criticality:** PII/결제 데이터 처리 여부에 따른 가중치
- **Reachability:** 인터넷에 노출된 코드인지 분석

Fix

개발자 워크플로우

- **Bi-directional Sync:** Jira 티켓 상태와 보안 도구 상태 자동 동기화
- **Dev-Friendly Details:** 재현 단계, 수정 코드 스니펫 포함
- **Auto Assignment:** 코드 소유자(Owner) 자동 식별 및 할당

Verify

지속적 위협 관리

- **Scheduled Scans:** 정기적인 자산 재스캔 자동화
- **CI/CD Gating:** 심각한 위험 발견 시 배포 파이프라인 차단
- **Drift Detection:** 보안 설정 변경 사항 자동 감지

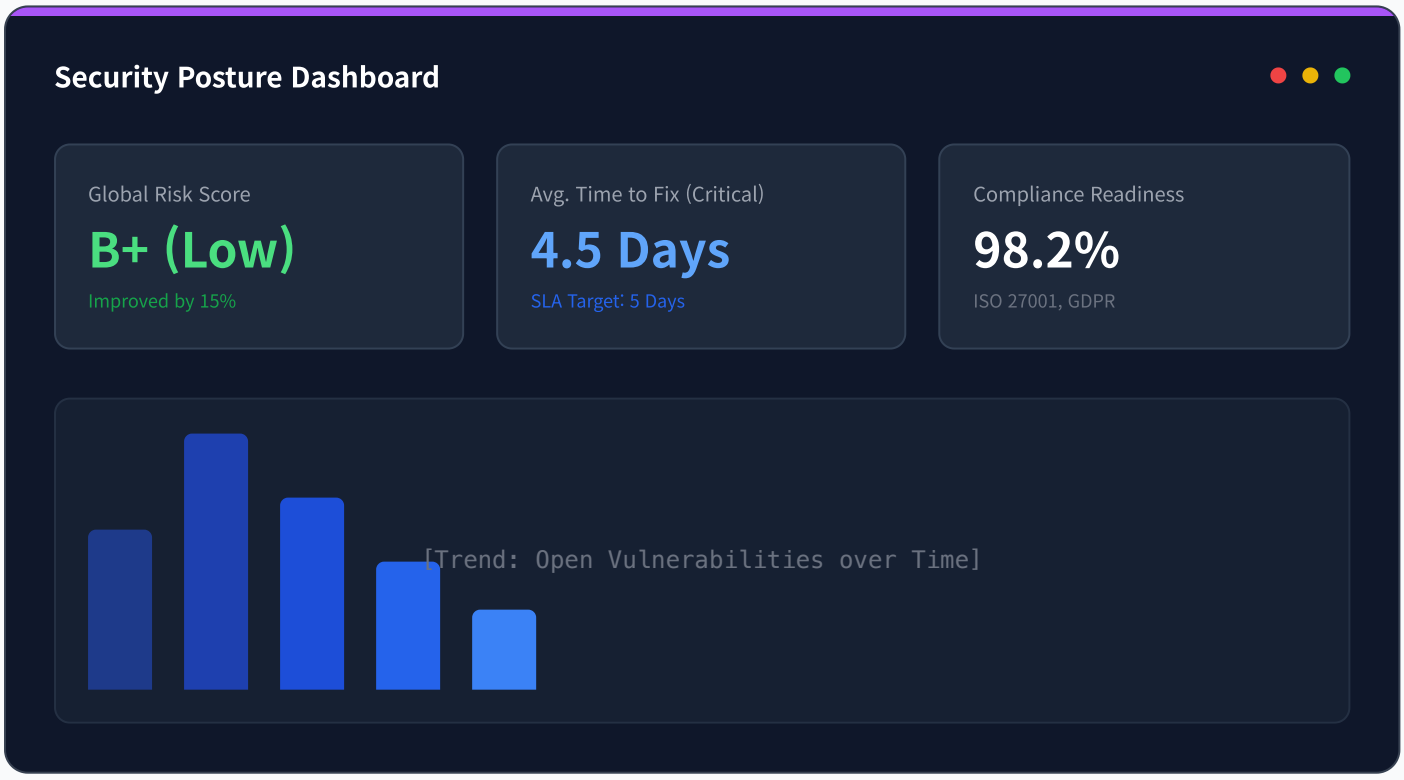
기능 (Feature)	전통적 AppSec	Invicti ASPM
Data View	파편화된 사일로 (Fragmented)	**통합된 단일 뷰 (Unified)**
Prioritization	단순 CVSS 점수 의존	**비즈니스 맥락 + EPSS + CVSS**
Remediation	수동 티켓 생성 및 추적	**양방향 자동 동기화**
Coverage	알려진 자산만 스캔	**동적 자산 식별 (Discovery)**

CISO'S CORNER

단순 숫자에서 실질적 위험 감소 지표로

경영진에게 "몇 개의 버그를 잡았는지"를 보고하지 마십시오.
Invicti ASPM은 비즈니스 리스크가 얼마나 감소했는지 보여주는 **전략적 KPI**를 제공합니다.

과거의 지표 (Vanity Metrics)	Invicti ASPM 지표 (Risk Metrics)
발견된 취약점 수 "5,000개 버그 발견." (그래서 우리가 안전한가요?)	**Risk Density (위험 밀도)** "애플리케이션당 심각한 위험이 평균 0.5개로 감소했습니다."
스캔 횟수 "100번 스캔했습니다." (중요 자산을 스캔했나요?)	**Asset Coverage (자산 커버리지)** "비즈니스 중요 자산의 100%가 7일 이내에 검증되었습니다."
전달된 티켓 수 "500개 전달." (개발팀이 실제로 고쳤나요?)	**MTTR & Fix Rate (조치 속도 및 율)** "치명적 위험의 MTTR이 5일로 줄었고, 수정율은 95%입니다."



💡 경영진(C-Suite)을 위한 전략적 가치

- **ROI 증명:** 자동화를 통해 절감된 인력 시간(Man-hours)과 비용을 수치화합니다.
- **규제 준수:** GDPR, PCI-DSS 등 컴플라이언스 상태를 실시간으로 확인합니다.
- **출시 속도 향상:** 보안 병목 현상을 제거하여 비즈니스 민첩성을 확보합니다.
- **브랜드 보호:** 데이터 유출 사고를 사전에 예방하여 기업 평판을 보호합니다.

선제적 보안의 새로운 기준

사후 대응이 아닌 **사전 예방**을 선택하십시오.
전 세계 3,600개 이상의 회사들이 **Invicti와 함께 해커보다 앞서** 나가고 있습니다.

PROVEN ROI

수동 점검 비용을 50% 이상 줄이세요

단순 반복 업무는 자동화하고,
보안팀은 전략에 집중하십시오.

FREE POC

우리 사이트도 될까? 직접 확인해 보세요

의심은 검증으로 바뀝니다.
2주간 무료로 성능을 체험하세요.

EXPERT SUPPORT

판매가 끝? 계속 지원합니다

벤더사 기술팀과 긴밀히 협력하여
사용하시는 동안 계속 돕습니다.

지금 바로 선제적 보안 체계 (Preemptive Security)를 완성하십시오.

eVolcano Inc.는 Invicti의 공식 파트너로서 벤더사와의 긴밀한 협력을 통해 **데모(PoC) 및 기술 지원**을 제공합니다.

WEBSITE	www.evolcano.co.kr
EMAIL	charliek@evolcano.co.kr
PHONE	070-4090-9400