TIER 3 · 실시간 API 가시화 · 명세 역공학 · 자율 가상 패치 보안 관제

2026.11 | Enterprise Edition v3.8

SyncAPIM

문서에 빠진 숨은 API를 실시간으로 찾아내고 재배포 없이 공격 차단과 개인정보 가림을 돕는 API 보안 관제

트래픽 분석으로 미등록 API와 타인 정보 순차 조회(BOLA) 시도를 빠르게 탐지하며,
정상 요청 200건 사전 검증을 거친 가상 패치로 코드 수정 전 방어 공백을 메웁니다.

핵심 제공 가치

숨어 있는 미등록 API 자동 발견

실제 트래픽을 분석해 문서에 없는 유령 API와 민감 정보 노출을 실시간 검출

재배포 없는 실시간 가상 패치

신규 해킹 공격 발견 시 서버 재시작 없이 차단 규칙만 즉시 적용(정상 요청 200건 사전 검증)

문맥을 아는 똑똑한 개인정보 마스킹

일반 주문번호는 건드리지 않고 실제 주민번호·카드번호·계좌번호만 정확히 가림

초경량 커널(eBPF) 서버·포트 감시

CPU 부담(0.3%) 없이 서버 내 몰래 열린 위험 포트와 취약 라이브러리를 감시

발행처 : 주식회사 엠파시 (Empasy Inc.) | 문의 : biz@empasy.io
문서 포털 : https://doc.empasy.com | 라이브 데모 : https://sync.empasy.io

SYNCAPIM CORE CAPABILITIES

핵심 구성 요약

01 실시간 API 자동 발견 & 명세 불일치 감사

유입되는 모든 API 트래픽을 자동 지도화하고 공식 OpenAPI 3.0 문서와 대조하여, 미등록 Shadow API와 미정의 민감 응답 필드를 찾아냅니다.

02 5대 지능형 인라인 방어 엔진 (< 1.0ms)

SQLi/XSS 구문 지문 분석, JWT 토큰 위변조 차단, 타인 데이터 순차 조회(BOLA) 차단, AI 프롬프트 탈옥 방화벽을 1ms 미만으로 수행합니다.

03 자연어 위협 검색 및 사전 검증 가상 패치

보안 담당자가 한글로 공격 로그를 검색하고, 정상 트래픽 200건 사전 검증을 거친 가상 패치를 무중단으로 반영합니다.

04 문맥 인지 개인정보 마스킹 & eBPF 자산 관제

응답 JSON의 키 이름과 값을 함께 분석해 주민번호·카드번호·시크릿키만 실시간 마스킹하고, Linux eBPF로 서버 포트와 네트워크 위협을 차단합니다.

기존 웹방화벽이 놓치기 쉬운 숨은 API와 문맥형 공격에 대응합니다

마이크로서비스와 모바일·AI 연동 API가 급증하면서 보안팀도 존재를 모르는 API가 해킹 통로가 되고 있습니다. API의 문맥을 이해하는 전용 보안 관제가 필수입니다.

현재 현장에서 겪는 어려움 (AS-IS)

01. 개발팀이 테스트용으로 열어둔 미등록 API가 방치됨

공식 API 문서에는 없지만 실제 서버에는 열려 있는 옛날 버전 API나 디버그 경로(Shadow API)를 보안팀이 일일이 찾을 방법이 없습니다.

02. 정상 로그인 후 남의 주문번호·계좌를 조회하는 공격(BOLA)

기존 웹방화벽은 특수문자 해킹만 막을 뿐, 정상 토큰을 가진 사용자가 번호만 바꿔가며 타인의 정보를 긁어가는 공격은 정상 요청으로 통과시킵니다.

03. 신규 취약점 발견 후 개발팀이 코드 패치할 때까지 무방비

긴급 보안 취약점이 터져도 개발팀이 코드를 수정하고 QA를 거쳐 재배포하기까지 수일 동안 해킹 공격에 그대로 노출됩니다.

04. 개발 실수로 API 응답에 주민번호·카드번호가 평문 노출

백엔드 코드 한 곳에서 마스킹 처리를 빠뜨리면 고객의 주민등록번호나 신용카드 번호가 응답 JSON과 로그에 그대로 흘러나갑니다.

SyncAPIM이 풀어내는 방식 (TO-BE)

01. 실제 트래픽 역공학으로 전사 API 목록 실시간 목록화

미등록 API 자동 탐지

들어오는 패킷을 실시간 분석해 전체 API 트리를 자동으로 그리고, 공식 명세서와 다른 미등록 API나 과다 노출 필드를 즉시 경보합니다.

02. 세션별 행위 분석으로 타인 데이터 열거(BOLA) 및 JWT 위조 차단

판정 지연 < 1.0ms

짧은 시간 안에 서로 다른 객체 ID(주문·계좌·회원번호)를 순차 조회하는 비정상 행위와 JWT 서명 우회 시도를 인라인에서 즉시 차단합니다.

03. 백테스팅 검증된 '실시간 가상 패치'로 재배포 없이 즉시 방어

200건 사전 검증 배포

공격 패턴을 막는 SpEL 방어식을 즉시 합성하고 기존 정상 요청 200건과 대조해 정상 요청에 영향이 없는지 확인한 뒤 무중단으로 빠르게 반영합니다.

04. JSON 키 문맥을 이해하는 실시간 개인정보(PII) 인라인 마스킹

응답 직전 자동 마스킹

residentRegNo, cardNumber 등 JSON 키 문맥과 숫자 패턴을 함께 인식해 주문번호 오탐 없이 실제 개인정보만 응답 직전에 마스킹합니다.

핵심 정리 SyncAPIM은 단순 API 중계기가 아니라, 모든 API를 스스로 찾아내고 문맥을 이해해 방어하는 '자율형 API 보안 관제 센터'입니다.

API 자동 파악 · 저지연 인라인 방어 · 응답 마스킹 · 가상 패치 흐름

업무 서버의 성능을 떨어뜨리지 않도록 초고속 인라인 게이트웨이 필터와 비동기 위협 분석·가상 패치 엔진을 분리해 설계했습니다.

SyncAPIM 4단계 처리 흐름 (요청 접수부터 사전 확인 · 실행 · 복원 준비까지)

STEP 01 · 자동 발견

API 트래픽 유입 & 가시화

유입되는 모든 API 경로와 파라미터 구조를 자동 카탈로그화하고 스펙 불일치를 감지합니다.

STEP 02 · 인라인 방어

5대 인라인 위협 차단 (<1ms)

구문 분석 SQLi/XSS, JWT 무결성, BOLA 열거, AI 프롬프트 탈옥 공격을 실시간 차단합니다.

확인 게이트 · 200건 리플레이 백테스팅

신규 가상 패치 규칙이 기존 정상 트래픽을 단 1건이라도 막는지 사전 검증(정상 요청 통과)

STEP 03 · 유출 차단

응답 개인정보(PII) 마스킹

백엔드 응답이 나가기 직전 주민번호·카드번호·계좌번호·비밀키를 문맥 기반으로 가립니다.

STEP 04 · 무중단 패치

자율 가상 패치 & eBPF 연동

신규 공격 패턴 발견 시 백테스팅 검증 후 게이트웨이와 커널(eBPF)에 즉시 차단 규칙을 배포합니다.

역할 분담 : AI가 맡는 부분과 담당자가 직접 결정하는 부분

AI 보안 에이전트 자동 수행 영역

API 발견 · 공격 차단 · 마스킹 · 패치 합성

- 미등록 Shadow API 및 명세에 없는 민감 응답 필드 실시간 검출
- 1ms 미만 인라인 공격 차단 및 응답 페이로드 내 8대 개인정보 마스킹
- 차단된 공격 패킷 분석 및 MITRE ATT&CK 전술 매핑 브리핑
- 공격 차단용 가상 패치 규칙 자동 합성 및 정상 트래픽 백테스팅

사람(보안 담당자) 결정 영역

가상 패치 최종 승인 및 정책 관리

- 자연어로 위협 로그 검색('오늘 차단된 결제 SQL 공격 보여줘') 및 분석
- 백테스팅(공격 탐지·정상 통과) 결과가 확인된 가상 패치의 운영 배포 승인
- 발견된 미등록 Shadow API를 공식 명세로 등록할지 차단할지 결정
- 도메인별 개인정보 마스킹 수준(부분 가림 / 전체 가림 / 해시) 지정

시스템 안전 장치 영역

사전 검증 및 저부하 커널 보호

- 정규식 무한 루프(ReDoS) 방지 및 안전한 Restricted SpEL 샌드박스 실행
- 정상 서비스 장애를 유발하는 오탐(False Positive) 규칙 배포 사전 차단
- CPU 오버헤드 0.29% 이하의 초경량 eBPF 센서로 서버 성능 영향 최소화
- SyncWatch와 연동해 전 세계 신규 CVE 공격 시그니처 상시 자동 업데이트

작동 원리 가장 까다로운 '오탐(정상 고객 요청을 잘못 막는 사고)' 문제를 정상 트래픽 200건 자동 리플레이 백테스팅으로 실무에 맞게 보완했습니다.

초당 API 트래픽 · 탐지된 공격 · 판정 속도 실시간 관제

활용 시점 : 보안 관제실이나 운영팀에서 현재 우리 API 서버들에 어떤 공격이 들어오고 있고 방어 엔진이 몇 밀리초(ms) 만에 처리하는지 볼 때 사용합니다.

주요 제공 기능

인라인 지연 < 1.0ms

01 실시간 API 요청량 · 차단 건수 · 인라인 판정 지연(< 1ms) 모니터

전체 API 호출 추이와 그중 차단된 악성 요청 비율, 방어 엔진의 초저지연 처리 속도를 실시간 차트로 한눈에 확인합니다.

02 5대 공격 유형별(SQLi · BOLA · JWT · AI 탈옥 · SSRF) 탐지 현황

어떤 종류의 공격이 어느 서비스 도메인(결제, 회원, 마이데이터 등)을 노리고 있는지 유형별로 명확하게 분류해 보여줍니다.

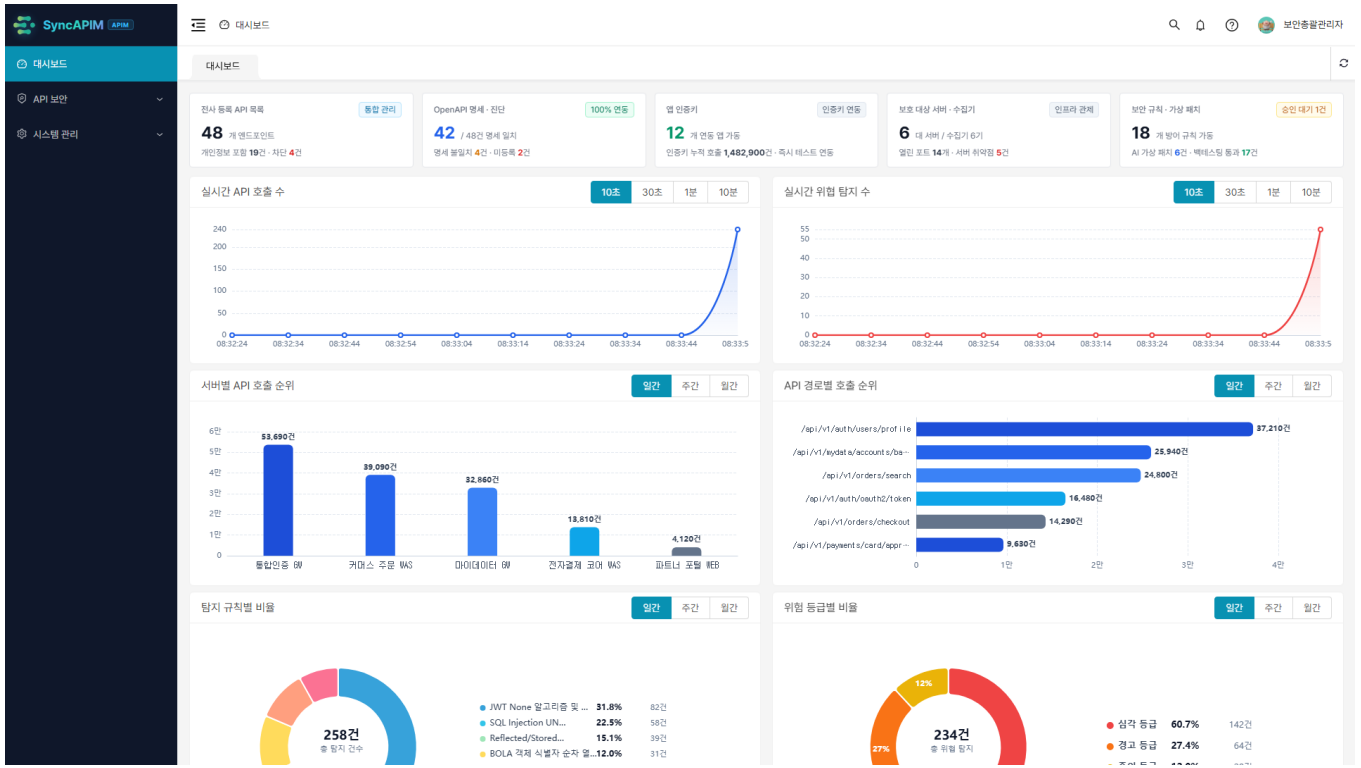
03 미등록 Shadow API 및 개인정보 마스킹 실시간 카운터

새로 발견된 미승인 API 건수와 응답에서 자동 마스킹되어 유출을 막아낸 개인정보 건수를 핵심 지표로 즉시 파악합니다.

04 최근 고위험 위협 경보 및 원클릭 상세 패킷 분석 이동

위험도가 높은 공격 시도를 상단 경보로 띄워 주고, 클릭 즉시 해당 패킷의 헤더·바디와 방어 규칙 화면으로 바로 연결합니다.

https://sync.empasy.io/apim/dashboard



구동 화면 | SyncAPIM 실시간 보안 관제 대시보드 — API 트래픽, 5대 위협 차단 현황 및 초저지연 성능 지표 (시연 데이터 기준)

실무 활용 속도 저하 때문에 보안 옵션을 꺼두어야 했던 기존 무거운 WAF와 달리, 1ms 미만의 처리 속도로 성능과 보안을 동시에 잡습니다.

트래픽 분석 기반 미등록 API 파악 및 명세 불일치 점검

활용 시점 : 사내에 실제로 열려 있는 모든 API 목록을 파악하거나, 개발팀이 문서 업데이트 없이 임의로 바꾼 API 응답 필드를 감사할 때 사용합니다.

주요 제공 기능

미등록 API 자동 목록화

01 실제 트래픽 기반 호스트 · URI 경로 트리 자동 구축

일일이 수기로 등록하지 않아도 게이트웨이를 통과하는 트래픽을 분석해 도메인별·메소드별(GET/POST/PUT/DELETE) API 지도를 자동 완성합니다.

02 미등록 유령 API (Shadow / Zombie API) 즉시 색출

공식 OpenAPI 3.0 문서에는 없는데 외부에서 호출되고 있는 테스트용·구버전 API에 경고 배지를 띄워 즉시 차단하거나 관리에 편입시킵니다.

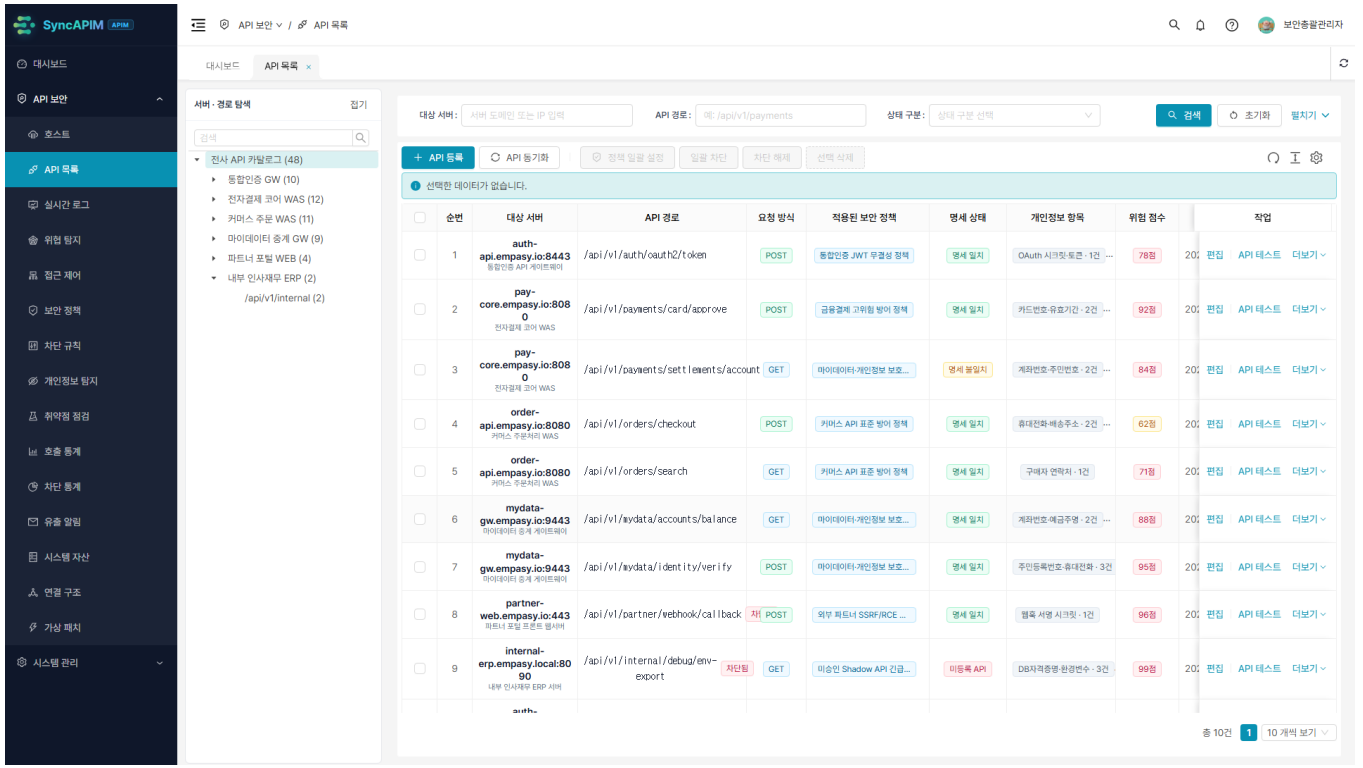
03 요청·응답 스펙 불일치(Spec Drift) 및 민감 필드 노출 진단

문서에는 없던 residentRegNo, internalToken 같은 민감 필드가 실제 응답 JSON에 실려 나가고 있으면 필드 단위로 정확히 집어냅니다.

04 실제 트래픽 역공학 기반 OpenAPI 3.0 명세서 자동 추출

문서가 아예 없는 레거시 시스템이라도 실제 오가는 요청·응답 구조를 역공학하여 표준 OpenAPI 3.0(Swagger) 명세서를 자동 생성해 줍니다.

https://sync.empasy.io/apim/endpoints



구동 화면 | SyncAPIM 엔드포인트 카탈로그 — 트래픽 역공학 기반 API 트리, Shadow API 및 스펙 드리프트 감사 (시연 데이터 기준)

실무 활용 보안의 첫걸음은 '우리 회사에 무엇이 열려 있는지 아는 것'입니다. 문서화되지 않은 사각지대 API를 단 하나도 남기지 않습니다.

한글 로그 검색 및 정상 요청 200건 사전 검증 가상 패치

활용 시점 : 새로운 해킹 시도가 포착되었을 때 공격 패킷을 상세히 해부하고, 개발팀이 코드를 고치기 전 게이트웨이에서 즉시 방어막을 칠 때 사용합니다.

주요 제공 기능

200건 리플레이 검증

01 한글 자연어 위협 헌팅 ('차단된 결제 SQL 공격 보여줘')

복잡한 로그 검색 문법을 몰라도 일상적인 한글 문장으로 원하는 시간대·공격 유형·대상 API의 위협 패킷을 즉시 찾아냅니다.

02 공격 패킷 원문 하이라이트 및 MITRE ATT&CK 전술 해설

해커가 보낸 헤더·쿼리·바디 중 어느 부분이 왜 위험한지 정확히 집어 주고, 공격 의도와 대응 플레이북을 알기 쉽게 설명합니다.

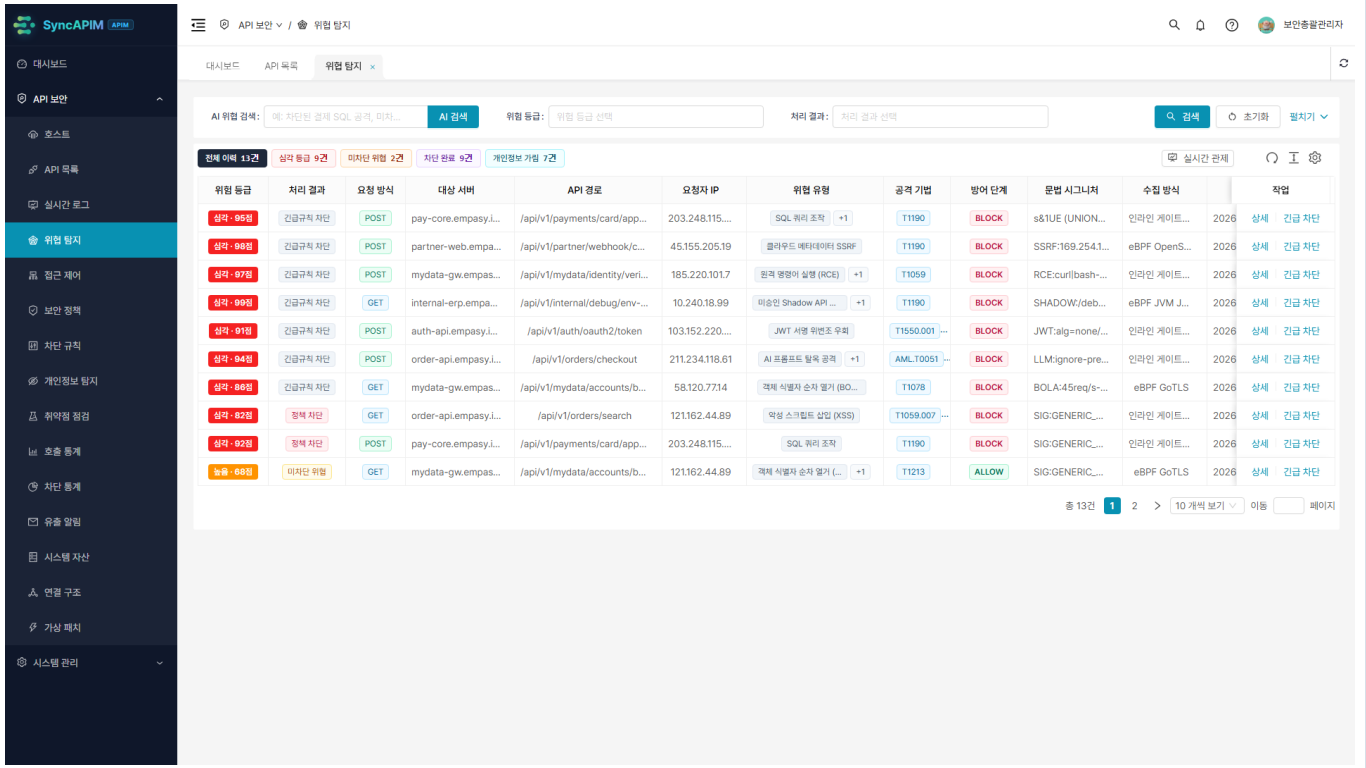
03 원클릭 가상 패치 방어식(Restricted SpEL) 자동 합성

해당 공격 패턴을 막는 정밀 방어 규칙을 AI가 즉시 작성해 주며, 정규식 서비스 거부(ReDoS) 안전성 검사를 자동으로 통과시킵니다.

04 정상 트래픽 200건 리플레이 백테스팅 후 무중단 핫리로드

배포 버튼을 누르기 전 실제 정상 요청 200건에 대입해 정상 요청을 막지 않는지 사전 검증한 뒤, 서버 재기동 없이 인라인 엔진에 빠르게 반영합니다.

https://sync.empasy.io/apim/threat-requests



구동 화면 | SyncAPIM 위협 헌팅 및 자율 가상 패치 — 공격 패킷 분석, 방어식 합성 및 200건 정상 트래픽 백테스팅 (시연 데이터 기준)

실무 활용 신규 취약점 발생 시 수일씩 걸리던 보안 패치 공백 시간을 '신속한 사전 검증 가상 패치'로 메워 제로데이 공격을 안정적으로 줄여 줍니다.

응답 문맥 기반 개인정보 가림 및 커널(eBPF) 서버 자산 점검

활용 시점 : API 응답으로 개인정보가 새어 나가지 않도록 보호 정책을 걸거나, 서버 호스트 내부의 미승인 오픈 포트와 통신 토폴로지를 감시할 때 사용합니다.

주요 제공 기능

eBPF CPU 부하 0.29%

01 JSON 키 문맥 + 값 패턴 결합으로 오탐 없는 개인정보 마스킹

단순 숫자 자릿수만 보지 않고 JSON 필드명 문맥을 함께 읽어, 일반 주문번호는 그대로 두고 주민번호·카드번호·계좌번호·시크릿키만 정확히 마스킹합니다.

02 부분 가림 · 전체 가림 · SHA-256 해시 등 유연한 마스킹 옵션

화면 표시용(010-****-5678), 비밀키 완전 숨김([REDACTED]), 로그 통계용 단방향 해시 중 업무 목적에 맞는 방식을 선택할 수 있습니다.

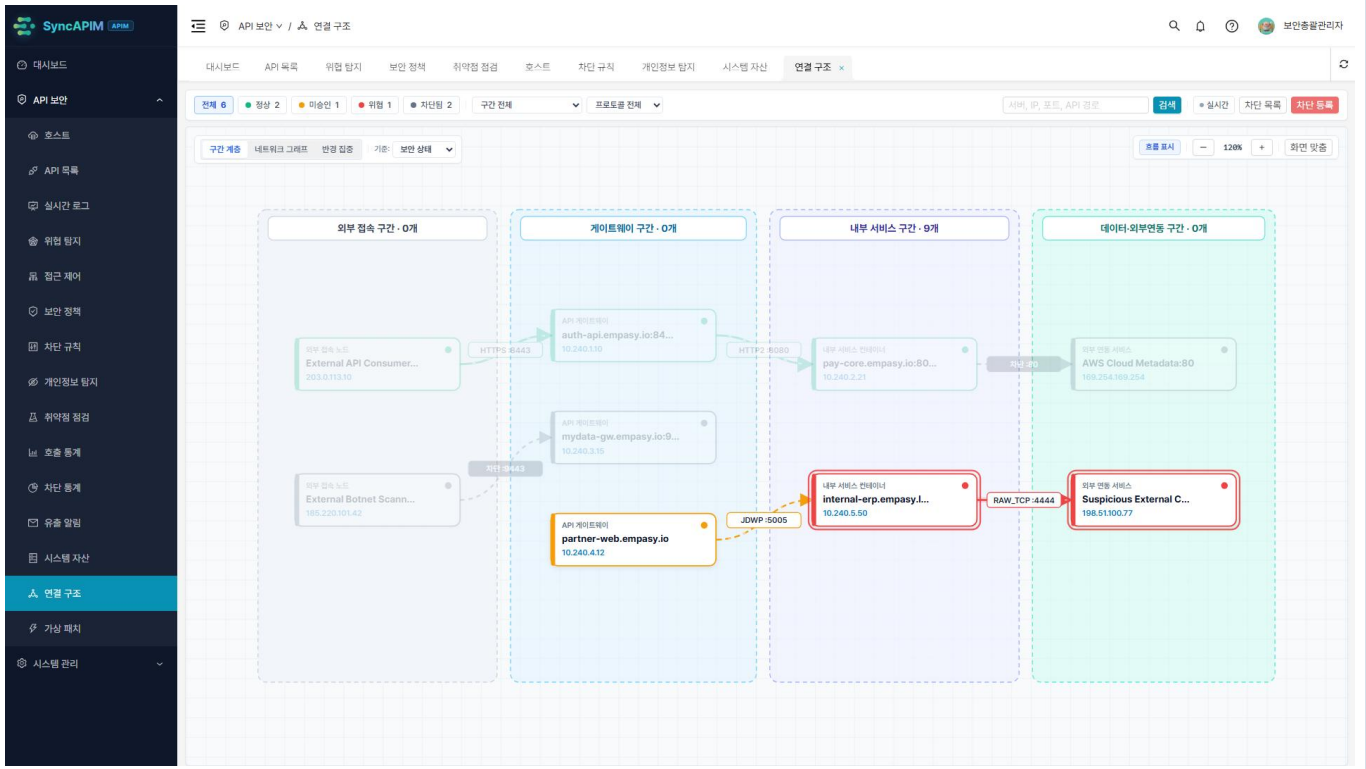
03 초저부하(CPU 0.29%) Linux eBPF 호스트 자산 및 오픈 포트 스캔

별도 코드 수정 없이 커널 eBPF 센서로 서버 내 열려 있는 포트, 몰래 열린 디버그 포트(JDWP/JMX), 실행 중인 라이브러리(SBOM) 취약점을 찾아냅니다.

04 L3/L4/L7 네트워크 토폴로지 가시화 및 커널 단계 즉시 드롭

내부 클라우드 메타데이터 탈취(SSRF 169.254.169.254)나 악성 봇넷 IP를 애플리케이션에 도달하기 전 커널(XDP/cgroup) 단계에서 즉시 차단합니다.

https://sync.empasy.io/apim/network-topology



구동 화면 | SyncAPIM eBPF 네트워크 토폴로지 & 자산 관제 — L3/L4/L7 트래픽 흐름 및 커널 단계 실시간 차단 (시연 데이터 기준)

실무 활용 애플리케이션 계층(L7 API 문맥 방어 및 PII 마스킹)과 운영체제 커널 계층(L3/L4 eBPF 방어)을 하나로 결합한 차세대 심층 방어 체계입니다.

정상 요청 200건 사전 검증과 성능 분리 설계로 오탐·지연 부담 완화

보안 도구가 오히려 운영 장애의 원인이 되지 않도록 성능 격리와 사전 오탐 최소화 검증을 철저하게 적용했습니다.

1차 안전망 · 사전 검증 — 200건 정상 요청 검증

정상 트래픽 200건 자동 리플레이 백테스팅 (공격·정상 샘플 사전 시험)

새로 만든 차단 규칙이나 SyncWatch에서 수신한 보안 룰은 반드시 실제 정상 트래픽 샘플 200건과 공격 샘플을 통과해 정상 요청을 막지 않는 것이 확인되어야만 운영에 적용됩니다.

2차 안전망 · 성능 격리 — 저지연 인라인 분리 설계

인라인 게이트웨이와 무거운 AI 분석 엔진의 물리적 격리

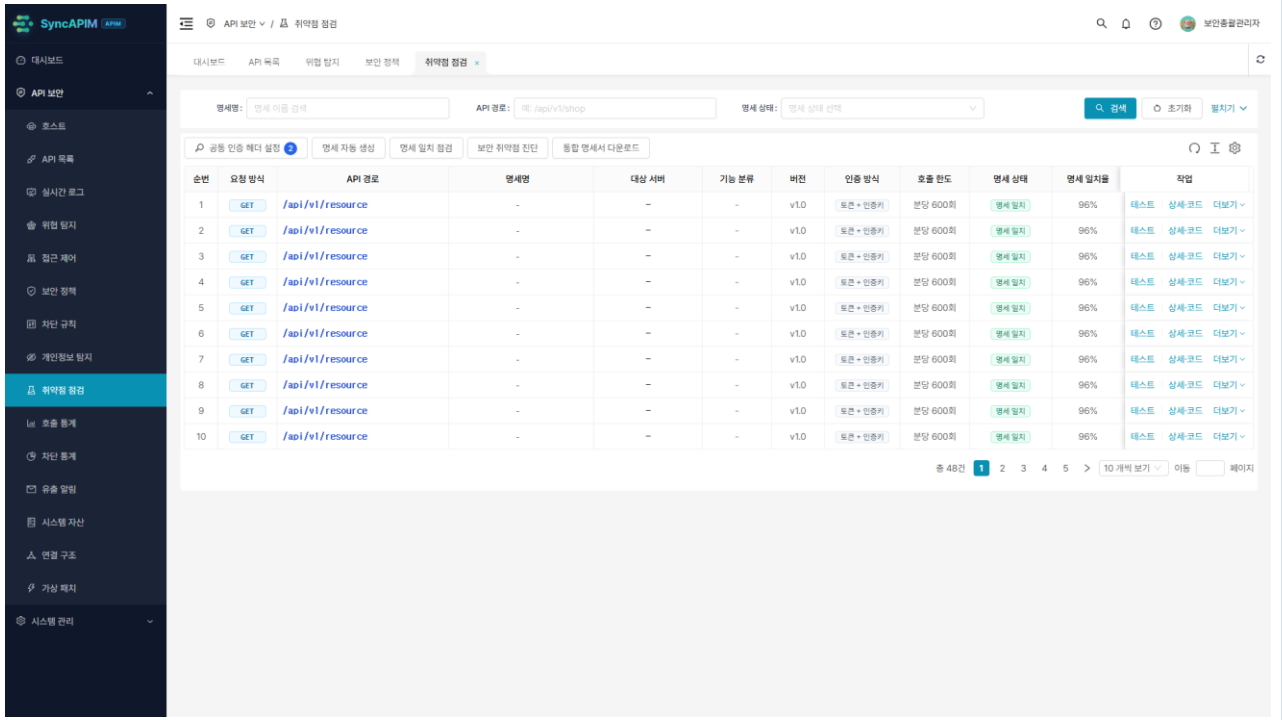
실제 고객 트래픽이 지나는 인라인 경로에서는 1ms 미만의 경량 구문 분석과 SpEL 평가만 수행하고, 무거운 AI 위협 분석과 리플레이 검증은 별도 격리 프로세스에서 비동기로 처리합니다.

3차 안전망 · 즉시 복원 — 빠른 정책 롤백

가상 패치 1-Click 비활성화 & Shadow(모니터링 전용) 모드 지원

신규 방어 규칙을 바로 차단(BLOCK)으로 걸기 부담스러울 때는 로그만 기록하는 감지(SHADOW) 모드로 먼저 돌려본 뒤 승격할 수 있으며, 언제든 즉시 해제할 수 있습니다.

https://sync.empasy.io/apim/virtual-patch



구동 화면 | SyncAPIM 가상 패치 백테스팅 및 배포 승인 모달 — 정탐/오탐 시뮬레이션 검증 결과 확인 (시연 데이터 기준)

안전 통제 — '일단 막고 보자'가 아니라 '정상 요청에 영향이 없는지 먼저 확인하고 정확히 공격만 막는다'는 엔터프라이즈 운영 원칙을 지킵니다.

기존 서버 앞단 게이트웨이 배치 및 SyncWatch 보안 규칙 자동 연계

백엔드 애플리케이션 소스코드를 한 줄도 수정할 필요 없이, 앞단 게이트웨이 또는 미러링 구성으로 즉시 도입할 수 있습니다.

방식 A. SyncAPIM 단독 도입 (기존 사내 시스템에 연결)

01. 코드 수정 없는 앞단 게이트웨이 / 리버스 프록시 즉시 배치

기존 Spring Boot, Node.js, Python, 레거시 WAS 앞단에 배치하는 것만으로 전사 API 자동 발견, BOLA 차단, PII 마스킹이 즉시 작동합니다.

02. 트래픽 미러링(방어 전 가시화 전용) 단계적 도입 지원

초기에는 실제 트래픽 흐름에 전혀 개입하지 않는 미러링 모드로 연결해 숨은 API 목록과 취약점부터 안전하게 파악할 수 있습니다.

03. 공식 OpenAPI 3.0(Swagger) 문서 자동 추출 및 최신화

오래되어 문서가 유실된 레거시 API들의 최신 명세서를 자동 생성하여 차세대 구축이나 파트너 연동 문서로 바로 활용합니다.

04. ISMS-P 및 개인정보보호법 컴플라이언스 즉시 충족

API 응답 및 로그 내 고유식별정보·금융정보 실시간 마스킹과 접근 감사 기록으로 보안 인증 심사 요건을 한 번에 해결합니다.

방식 B. SyncSeries 연계 확장 (MCP 표준 에이전트 협업)

SyncWatch 연동 — **신규 글로벌 해킹 위협 -> 1분 내 가상 패치 자동 수신**

SyncWatch가 KISA·CISA·NVD에서 신규 취약점 공격 패턴을 수집·컴파일하면 SyncAPIM이 즉시 받아 백테스팅 후 가상 패치로 방어합니다.

SyncVerse 연동 — **가상 패치로 응급 방어 + 근본 소스코드 패치 PR 동시 진행**

SyncAPIM이 앞단에서 공격을 실시간 막아주는 동안, SyncVerse는 백엔드 원본 코드의 취약점을 고치는 PR을 자동 생성해 근본 원인을 제거합니다.

SyncETA 연동 — **배포 전후 API 보안 퍼징(Fuzzing) 및 모의해킹 자동 검증**

SyncETA가 비정상 파라미터와 권한 우회 시나리오로 API를 자동 점검하고, SyncAPIM이 이를 정확히 탐지·차단하는지 상시 검증합니다.

SyncLLM 연동 — **대고객 AI 챗봇 API의 프롬프트 탈옥(Jailbreak) 방화벽**

외부 고객에게 공개된 AI 서비스 API 앞단에서 시스템 프롬프트 유출 유도나 악성 명령 주입 시도를 실시간으로 걸러냅니다.

유연한 도입 | 탐지(SyncWatch) -> 즉각 가상 패치 방어(SyncAPIM) -> 근본 코드 수정(SyncVerse) -> 재검증(SyncETA)으로 이어지는 완결형 자율 보안 체계입니다.

보이지 않던 API 현황을 드러내고 신규 취약점 대응 공백을 크게 줄입니다

정적 정규식에만 의존하던 구형 웹방화벽의 한계를 넘어, API 문맥과 데이터 흐름을 이해하는 지능형 방어 체계로 전환합니다.

인라인 보안 판정 지연	신규 취약점 가상 패치	응답 개인정보 평문 노출	eBPF 호스트 센서 부하
< 1.0 ms	**수일 -> 1분**	**문맥 마스킹**	**0.29%**
Restricted SpEL & 구문 지문 분석	재배포 없는 백테스팅 핫리로드	응답 전 개인정보 가림	초경량 커널 포트·SBOM·XDP 관제

비교 항목	기존 방식 (AS-IS)	SyncAPIM 적용 후 (TO-BE)	예상 개선 변화
API 자산 파악	엑셀이나 오래된 Swagger 문서에 의존해 미등록·구버전 API 방치	실제 유입 트래픽 역공학으로 Shadow API 및 스펙 드리프트 실시간 탐지	**미등록 API 가시화**
타인 정보 탈취(BOLA)	정상 로그인 토큰만 있으면 주문·계좌번호 순차 변경 조회를 막지 못함	세션별 객체 식별자 열거 행위 및 JWT alg:none 위변조를 인라인에서 즉시 차단	**권한 외 조회 탐지·차단**
긴급 취약점 패치	개발팀 코드 수정 -> QA -> 정기 배포까지 수일간 해킹 공격에 노출	정상 트래픽 200건 사전 검증을 거친 가상 패치로 1분 내 무중단 방어	**대응 공백 대폭 단축**
개인정보(PII) 유출	개발자가 코드에서 마스킹을 누락하면 응답 JSON에 주민·카드번호 노출	JSON 키 문맥과 패턴을 함께 읽어 응답 반환 직전에 8대 민감정보 자동 마스킹	**평문 노출 사전 예방**
서버·네트워크 관제	무거운 보안 에이전트 설치로 서버 CPU 부하 증가 및 L7/커널 단절	저부하 eBPF 센서로 미승인 포트·SBOM 취약점·SSRF 커널 차단 통합	**서버 부하 90% 절감**

기대 효과 | 개발 속도를 늦추지 않으면서도 보안팀이 원하는 최고 수준의 API 가시성과 무중단 방어력을 동시에 확보할 수 있습니다.

트래픽 관찰 모드부터 인라인 가상 패치까지 4주에 걸쳐 안전하게 적용

초기 도입 시 기존 서비스에 어떠한 영향도 주지 않는 관찰(Shadow) 모드로 시작하여 검증 후 차단 모드로 단계적 전환이 가능합니다.

1. 현업 부담을 줄이는 4단계 점진 도입 절차

STEP 01 | 1주차
게이트웨이 연동 및 전사 API 자동 발견
트래픽 연결, 전사 API 엔드포인트 카탈로그 자동 생성 및 미등록 Shadow API·스펙 불일치 진단

STEP 02 | 2주차
문맥 인지 개인정보(PII) 마스킹 적용
응답 페이로드 내 주민번호·카드번호·계좌번호·시크릿키 실시간 마스킹 정책 적용 및 감사 로깅

STEP 03 | 3주차
5대 인라인 방어 엔진 & 자율 가상 패치 가동
SQLi/XSS 구문 지문, JWT 무결성, BOLA 탐지, AI 프롬프트 방화벽 및 200건 백테스팅 가상 패치 활성화

STEP 04 | 4주차~
eBPF 커널 센서 및 SyncWatch 자율 보안 루프
호스트 eBPF 오픈 포트·SBOM·XDP 차단 연동 및 SyncWatch 신규 위협 시그니처 자동 수신 체계 가동

2. 권장 서버 하드웨어 사양 (온프레미스 / 클라우드 공통)

구성 구분	권장 CPU · 메모리 · 디스크 및 적용 대상
소규모 / 단일 도메인	4 vCPU / 16GB RAM / 100GB SSD (일일 API 호출 1,000만 건 이하 인라인 방어 및 PII 마스킹)
전사 표준 운영형	8 vCPU / 32GB RAM / 300GB NVMe SSD (4-JVM 성능 격리 아키텍처 + PostgreSQL 18.6 + Redis 7.4)
대용량 고가용성(HA)	게이트웨이 노드 2대+(각 16 vCPU/32GB) Active-Active 구성 + 위협 분석 워커 분리
eBPF 호스트 센서	Linux Kernel 5.8+ (RHEL 8/9, Ubuntu 20.04/22.04/24.04) — 호스트당 CPU 0.3% 미만, 메모리 50MB 미만

3. 표준 기술 사양 및 호환 환경

기술 영역	적용 기술 및 지원 규격
백엔드 & 방어 엔진	Java 25 (JDK 25), Spring Boot 3.5, Spring Cloud Gateway, Restricted SpEL Sandbox, SqlXssLexicalTokenizer
데이터베이스 & 캐시	PostgreSQL 18.6 (pgvector 위협 캠페인 클러스터링 & 감사 원장), Redis 7.4 (정책 핫리로드 & BOLA 윈도우)
커널 센서 & 프로토콜	Linux eBPF (kprobe/uprobe, cgroup/connect4, TC, XDP), OpenAPI 3.0.1 역공학, JSON-RPC 2.0 MCP
프론트엔드 콘솔	Vue 3.5, TypeScript 5, ECharts 실시간 위협 토폴로지, 패킷 Diff 뷰어, 자연어 헌팅 콘솔

도입 지원 기존 시스템 수정 없이 앞단에 얹는 것만으로 API 자산 관리, 차세대 WAF, 개인정보 DLP, 커널 eBPF 보안을 한 번에 완성합니다.

EMPASY SYNCSERIES · SYNCAPIM

숨은 API를 파악하고 재배포 전에도 빠르게 방어 규칙을 적용하는 환경, SyncAPIM이 실무에 부담 없는 API 보안 관제를 지원합니다.

라이브 데모 포털(https://sync.empasy.io)에서 API 자동 발견 카탈로그와 사전 검증 가상 패치 백테스팅 화면을 직접 체험해 보세요.

01. 서비스 속도 저하 없는 1ms 방어

인라인 게이트웨이와 무거운 AI 분석 엔진을 철저히 격리하여 고객 체감 지연 없이 실시간으로 공격을 차단합니다.

02. 정상 요청을 지켜내는 사전 검증

모든 가상 패치 규칙은 실제 정상 트래픽 200건 사전 검증을 통과한 뒤에만 안전하게 적용됩니다.

03. 개인정보 평문 유출 사전 예방

개발자가 코드에서 마스킹을 빠뜨려도 게이트웨이가 응답 문맥을 읽어 주민번호·카드번호·계좌번호를 마지막 관문에서 지켜냅니다.

라이브 데모 체험 : https://sync.empasy.io | 문서·제안서 포털 : https://doc.empasy.com
도입 상담 및 2주 시범 적용(PoC) 문의 : 주식회사 엠파시 솔루션아키텍처팀 | biz@empasy.io