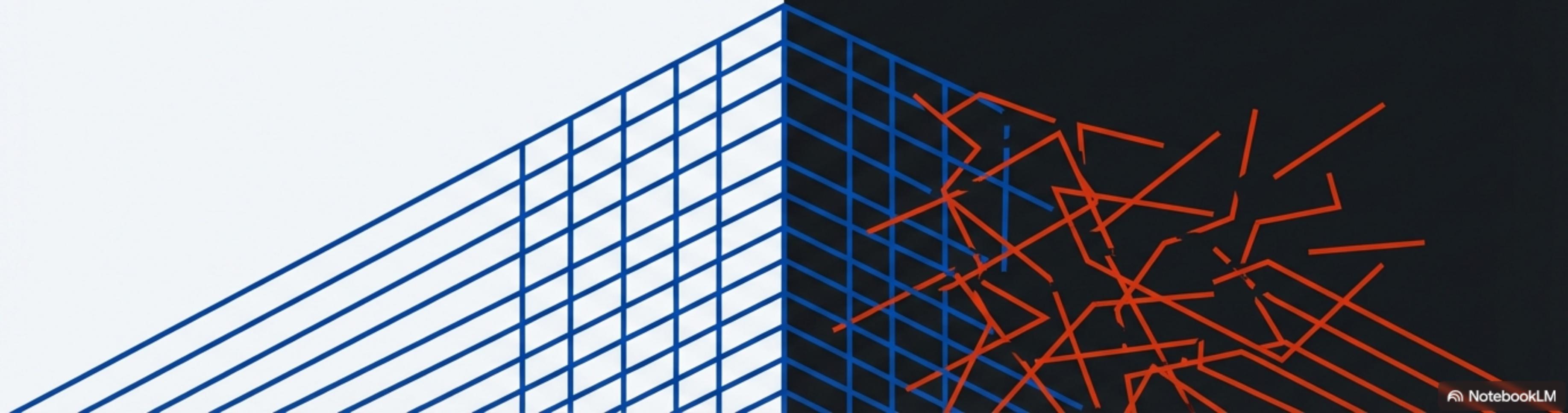


ASM, 2025년의 약속과 현실

공격 표면 관리는 왜 보안 담당자를

ASM, 2025년의 약속과 현실

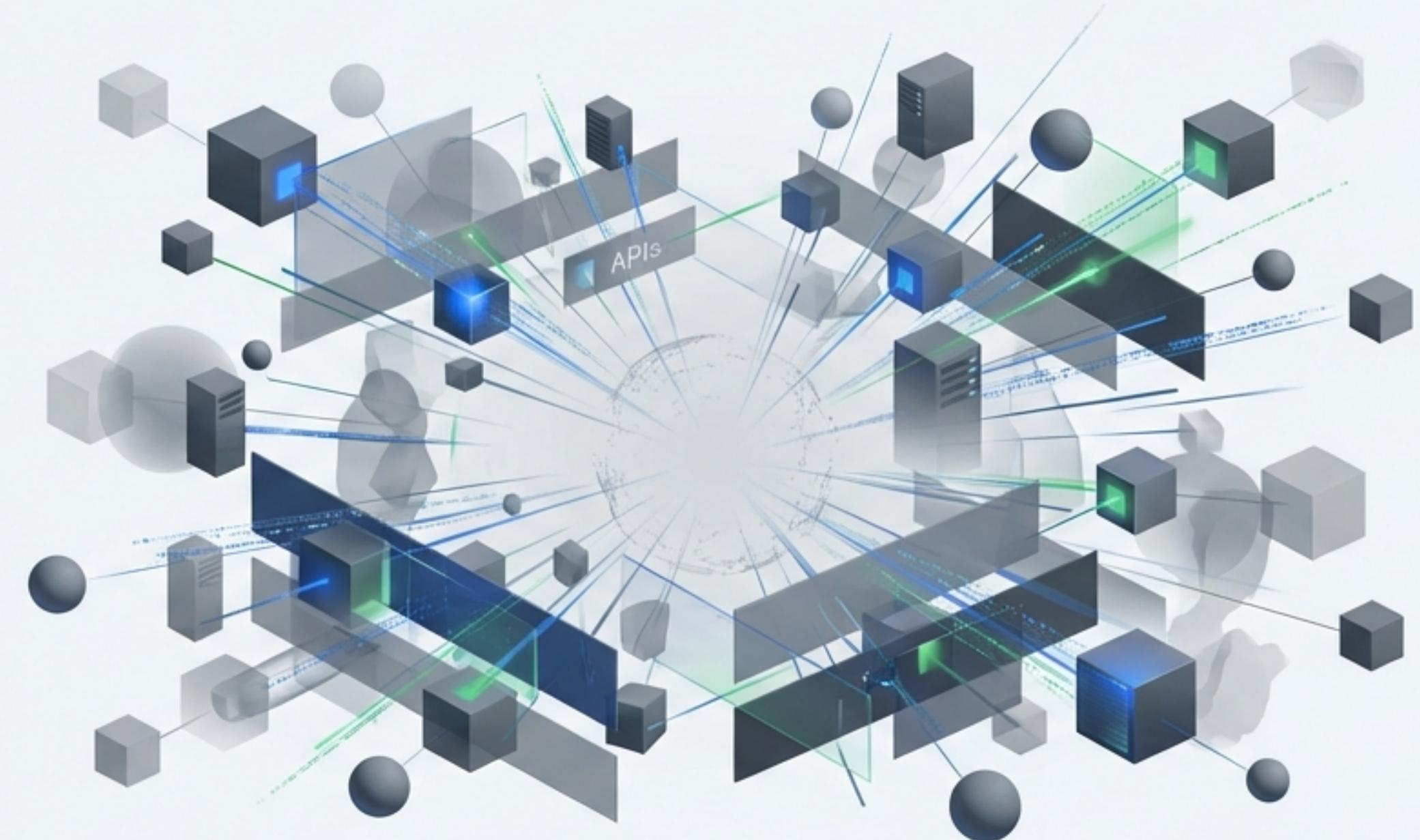
여전히 화나게 화소 나게 하는가



2025년, 공격 표면은 모든 곳에 존재합니다

전통적인 네트워크 경계는 사라졌습니다.
클라우드, SaaS, IoT, API가 자산의
지도를 무한히 확장시키고 있으며,
공격자는 AI를 이용해 단 몇 초 만에
취약점을 찾아냅니다.

“보이지 않는 것은
방어할 수 없다.”



92% 의 기업이 멀티 클라우드를 사용하며 복잡성을 가중시키고 있습니다.

ASM, ‘선택’이 아닌 ‘필수’가 되다



1. 디지털 확장 (Digital Expansion)

섀도우 IT와 빠른 서비스
배포로 인한 가시성 격차 발생



2. 동적 환경 (Dynamic Environments)

매일같이 생성되고 사라지는
클라우드 자산과 API



3. 진화하는 위협 (Advanced Threats)

AI 기반 공격의 가속화 및
API 취약점 급증.

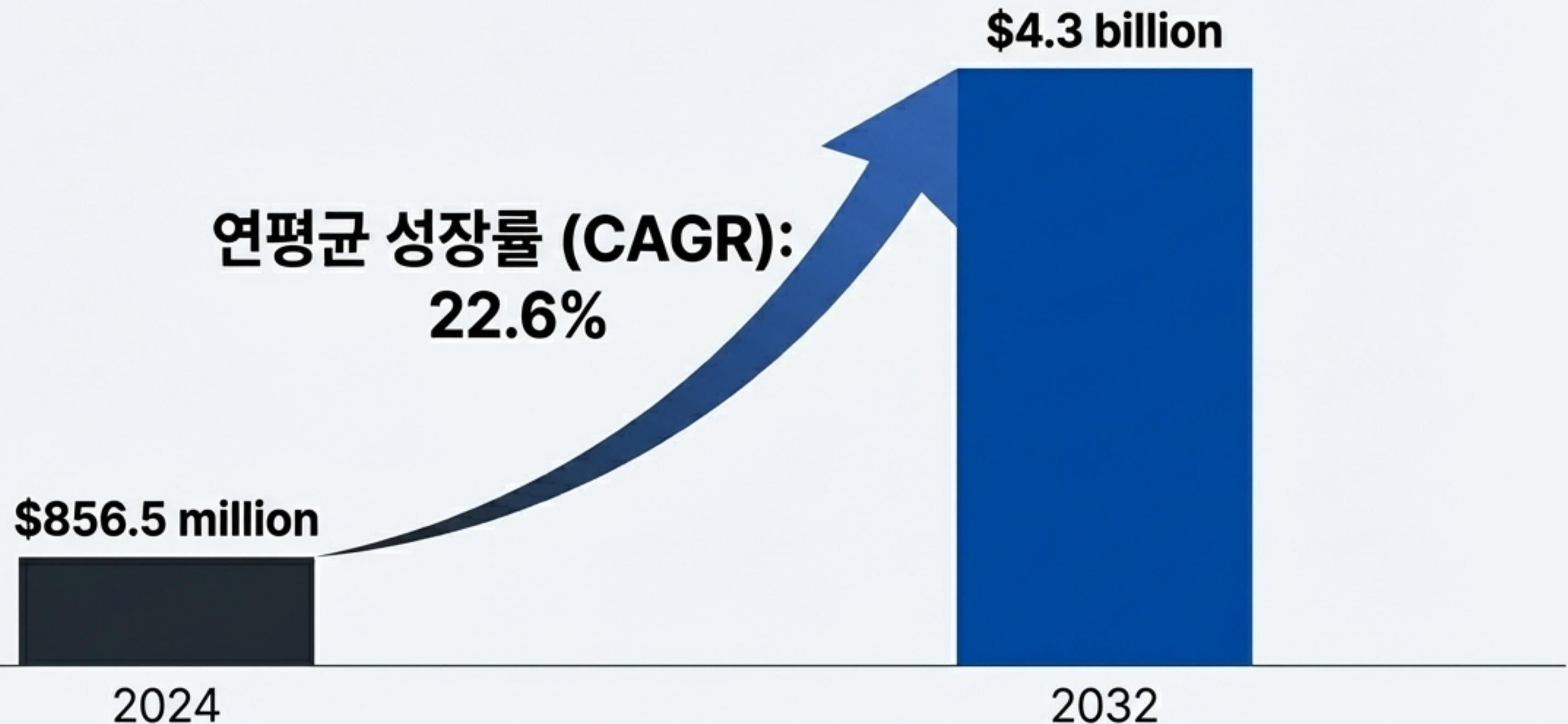
지난 1년간 **99%**의 기업이
최소 1회 이상의 API 보안
사고를 경험했습니다.



4. 규제 및 신뢰 (Compliance & Trust)

SEC 사이버 공시 규칙,
EU NIS2 등 자산 모니터링
의무화.

시장은 ASM의 가치를 증명합니다



시장의 폭발적인 성장은 ASM이 현대 비즈니스에서 필수적인 리스크 관리 도구로 인식되고 있음을 보여줍니다.

ASM은 AI와 만나 끊임없이 진화 중입니다

AI 기반 탐지 (AI-Powered Discovery)

자동화된 자산 발견 및
리스크 우선순위 지정

서드파티 리스크 모니터링 (Third-Party Risk Monitoring)

파트너 및 공급망의
공격 표면까지 관리 확장

제로 트러스트 통합 (Zero Trust Integration)

지속적인 자산 데이터로 'Never trust,
always verify' 원칙 지원

위협 인텔리전스(CTI) 연동 (Threat Intelligence Feeds)

실제 공격 시나리오 기반의
취약점 우선순위 결정

클라우드 및 API 커버리지 (Cloud & API Coverage)

멀티 클라우드 환경 전반의 자산 인벤토리 관리



하지만 현장에서는 다른 이야기가 들려옵니다

그래서, 이 모든 기술이 정말 공격을 막았는가?

문제 1: ASM은 구조적으로 느리다

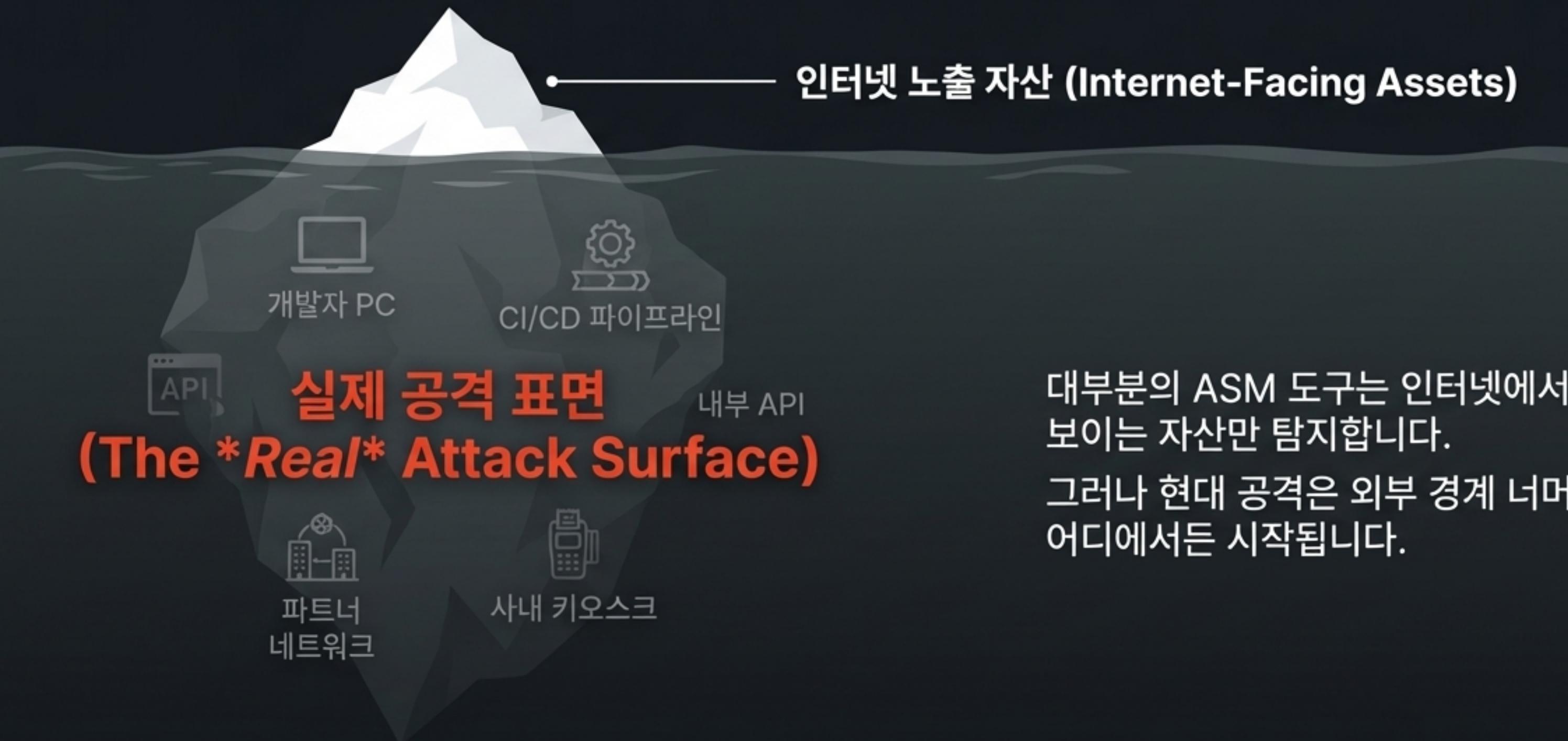
공격은 '분' 단위, ASM은 '주' 단위



문제는 기술이 아닌 운영 모델에 있습니다. ASM은 실시간 대응이 아닌 사후 보고를 위해 설계되었습니다.

문제 2: ASM은 세상을 1차원으로 본다

당신의 ASM은 ‘공격 표면’이 아닌 ‘외부 자산 목록’을 보고 있습니다.



문제 3: ASM은 결과물만 볼 뿐, 행위는 보지 못한다

취약한 URL 1개 vs. 취약점을 만드는 프로세스 1개



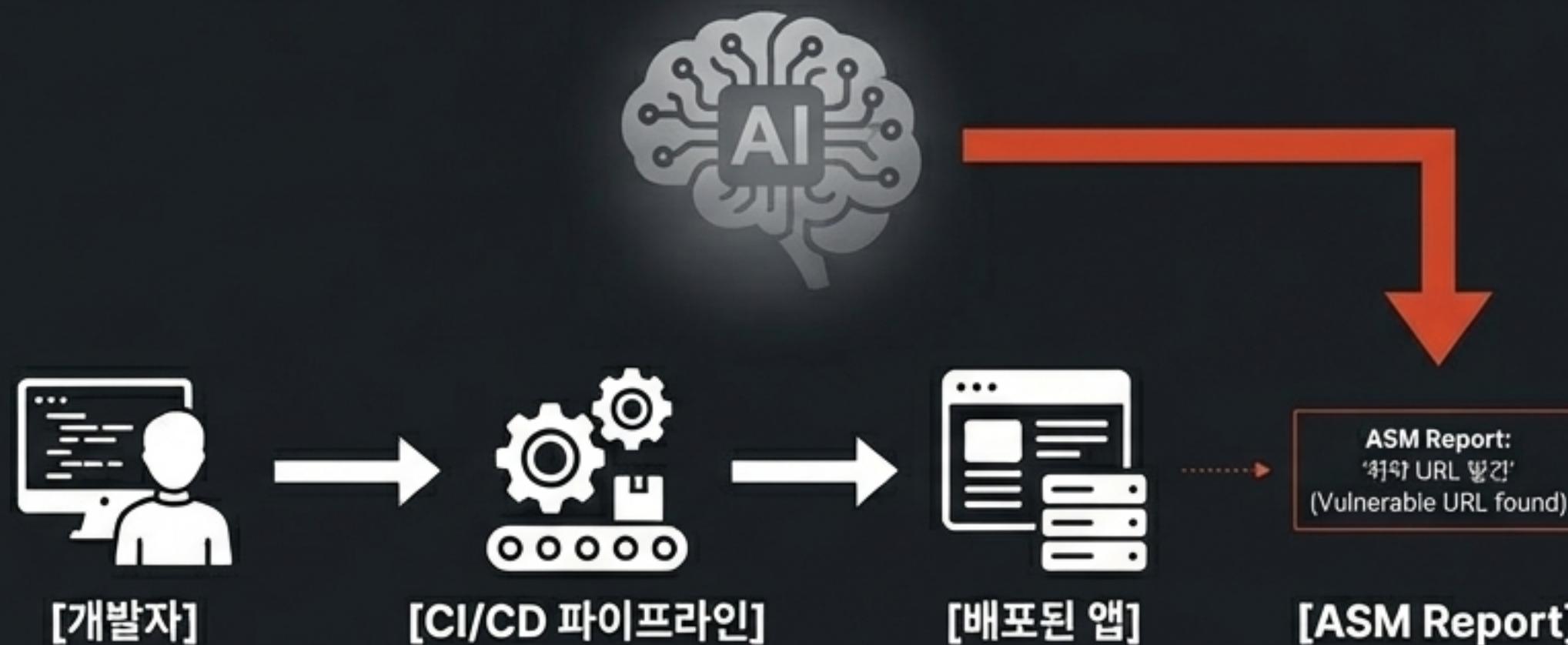
[개발자가 검증되지 않은 패키지 사용]
(Developer uses unvetted package)

[CI/CD 파이프라인 배포]
(CI/CD Pipeline deploys)

ASM Report:
'취약 URL 발견'
(Vulnerable URL found)

“ASM은 결과만 볼 뿐, 행위는 보지 못한다.”

“AI 기반 ASM”은 이 문제를 해결했는가? AI는 ‘나열’을 더 잘하게 만들었을 뿐입니다.



AI는 탐지 속도와 정확도를 향상시킬 수
– 있지만, 운영 모델이 변하지 않으면
근본적인 문제는 해결되지 않습니다.

더 빠르고, 1차원적이며, 결과물에만
집중된 보고서를 전달할 뿐입니다.

“AI가 보안 담당자의 금요일을 구해주지는 못했다.”

패러다임 전환: 자산이 아닌 ‘행위’를 관리하라

자산 중심
(Asset-Centric)

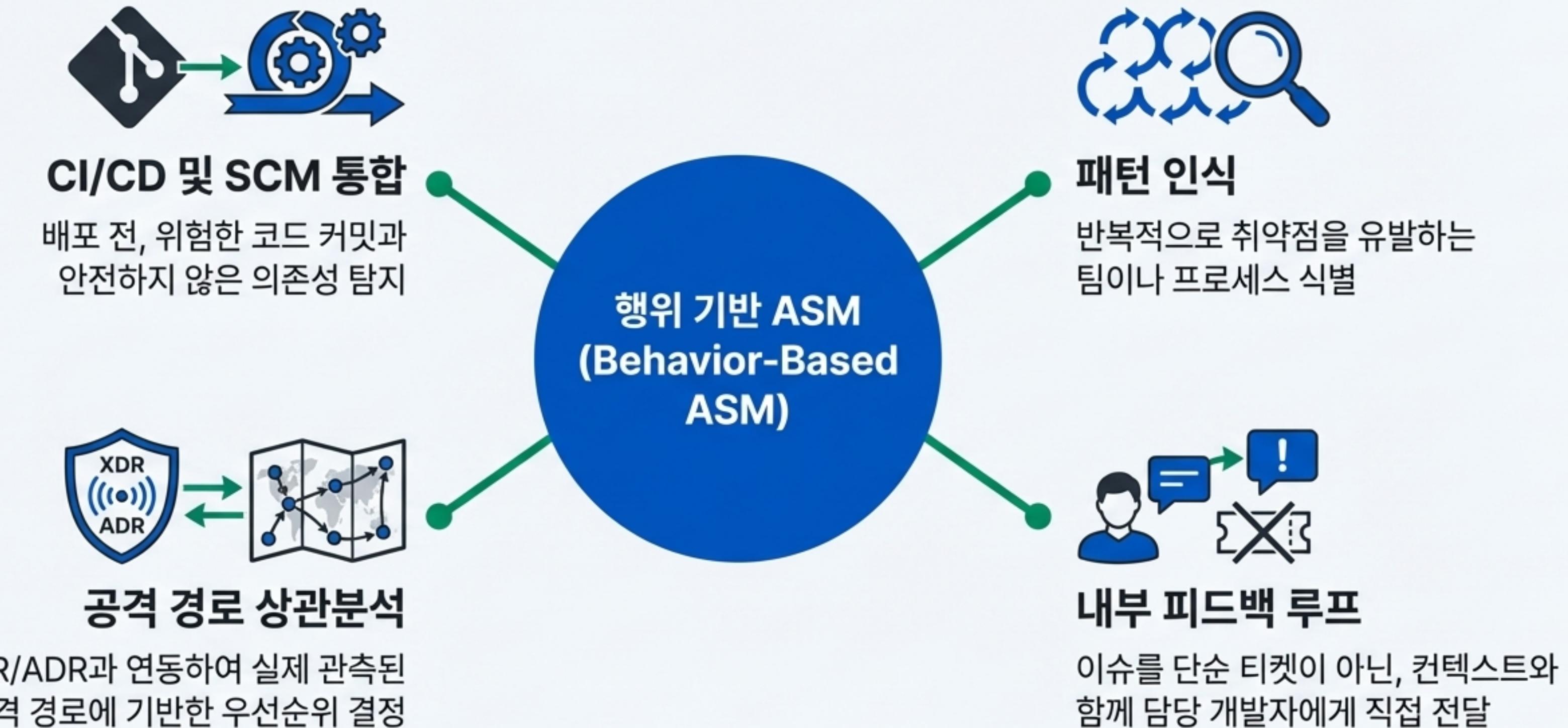


행위 중심
(Behavior-Centric)

공격 표면 (Attack Surface)은 자산 목록이 아니라,
리스크를 만들어내는 행위의 총합입니다.

취약점 관리 (Vulnerability Management)는 URL 패치가 아니라,
개발 습관과 파이프라인을 관리하는 것입니다.

행위 기반 ASM의 핵심 요소



Before & After: ASM의 진화

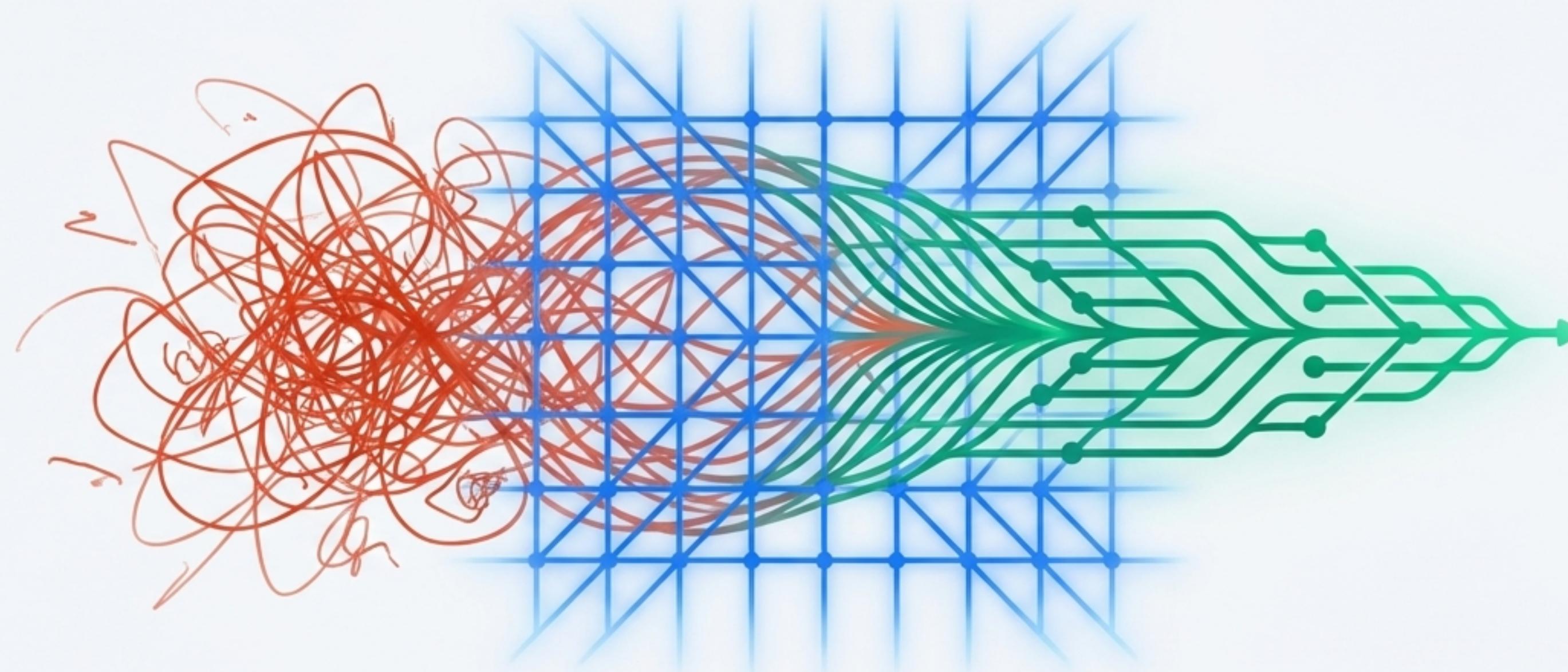
OLD MODEL (자산 나열 / Asset Listing)



NEW MODEL (행위 관리 / Behavior Management)



진짜 보안은 '착각'이 아닌 '체계'에서 시작됩니다



ASM 시장이 성장하는 이유는 문제가 실재하기 때문입니다. 그러나 현재의 ASM 형태는 "보안이 잘 되고 있다"는 잘못된 안도감을 제공할 뿐입니다. ASM의 진정한 진화는 수동적인 자산 목록 도구에서 벗어나, 우리가 기술을 만들고 운영하는 방식 그 자체의 구조를 관리하는 능동적인 시스템으로 거듭나는 것에 있습니다.

**자산을 나열하는 도구를 넘어,
공격을 만들어내는 구조를 관리하는 체계로.**