㈜스텔스솔루션 STEALTH SOLUTION

AI 자동 해킹 '능동방어'가 해답

"실증 마친 비책" 스텔스캐슬 (SMTD)

Stealth Moving Target Defense



AI 자동 해킹, 공격은 시작됐습니다

금융권 전반으로 확산, '업종불문' 기업도 비상

2026년 9월~11월 해킹 피해 (신고 기준)

금융사

37곳

은행·증권·보험 등
약 47만 건 데이터 유출

기업

11만곳

ERP 기업 해킹, 고객사 영향권
플랫폼·건설·화장품 등 업종불문

해외

8조원

바이낸스 해킹 피해

출처: 뉴스1 2026-11-06(금융권 37곳·47만 3천 건); 서울경제 2026-10-26(ERP); TRM Labs 2026-10-29(바이낸스)

외부와 연결하는 '접점'이 'AI의 공격 통로'입니다.

회사	해킹 경로(뚫린 외부 접점)
AA 은행	직원·모집인 등 외부 접속망 — AI 침투 에이전트(ARTEX) 활용
BB 증권	외부 협력사 접속망 — 정상 신호로 위장한 대규모 트래픽
CC 코인거래소	외주 업체가 운영하는 모바일 그룹웨어 — 고객·임직원 정보 유출
DD ERP기업	직원 VPN 탈취 — 개발 서버·백업 서버 침투
바이낸스	엔지니어 노트북 원격 접근 → 핫월렛 출금

당국 요구는 '외부 접점 전수점검 · 제로트러스트'입니다.
스텔스캐슬은 이 요구를 하나의 제품으로 구현합니다.

주: ARTEX: 딥시크 등 외부 LLM을 엮는 오픈소스 침투 에이전트
출처: 쿠키뉴스 2026-10-14; YTN 2026-10-28; SBS Biz 2026-10-29; MTN 2026-10-26; Al Jazeera 2026-10-30; 파이낸셜뉴스 2026-10-07

AI 자동 해킹, 왜 위험한가?

AI가 새로운 수법으로 공격한 건 아닙니다.
더 싸게, 더 빠르게, 더 많이 공격했을 뿐입니다

AI가 수행한 전술 작업

80~90%

사람은 결정점 4~6곳만

비전문가 재현

6분

공개 모델·GPU 1장

침투 확산 최단

27초

사람의 관제보다 빠름

→ **누구나, 쉽게, AI로, 24시간 해킹이 가능한 '위험한 세상'**

출처: Anthropic 위협 보고 2025-11-13; ZDNet Korea 2026-10-06(숭실대 가상실험); CrowdStrike 2026 Global Threat Report

벽을 쌓는 보안은 못 막습니다

방화벽·IDS·탐지
탐지 후 차단 — 사후입니다

- 침투를 확인한 뒤에야 차단
- 규칙 아래 소량 침투 시도는 통과

고정 IP·포트
지도가 공개돼 있습니다

- 주소가 그대로라 해커의 정찰에 공격지점 노출
- 일부 금융사는 공격 IP 공유 뒤에야 인지

탐지에 앞서, 공격자가 입구를 찾고 두드리지 못하게 하는 접근이 필요합니다

출처: 금융권 능동보안 제안서(2026-10); 뉴데일리 2026-10-08; Zscaler 10-K FY2026; morphisec.com; NIST SP 800-160 Vol.2 Rev.1

AI 자동 해킹 방어, '스텔스캐슬'(SMTD)이 왜 "비책"인가?

AI해커도 '찾을 수 없는 대상'을 공격할 수는 없습니다
스텔스캐슬은 숨기고, 믿지 않고, 격벽을 칩니다

출처: 금융권 능동보안 제안서(2026-10); 회사 및 기술소개 자료(2026-10)

'스텔스캐슬' 비책① 1초마다 주소를 바꿉니다.
(보호 자산 앞단에서 IP·Port 변이)

기존 보안-고정 표적

주소가 그대로입니다

- 한 번 찾은 IP·포트가 계속 유효

→

스텔스캐슬-움직이는 표적

주소가 계속 바뀝니다

- IP·포트를 **최대 1초** 단위로 변이

공격 표면 찾을 확률 1/42억

- 설령 찾아도 1초 후에 또 변경
- 이론상 조합 — 고객 실제 IP 대역·포트 기준 재산정

주: 변이는 SMTD 게이트웨이 외부 인터페이스에서 종단 — 후단은 기존 주소, 방화벽 정책 변경 없음

출처: 회사 및 기술소개 자료(2026-10)

'스텔스캐슬' 비책② 누구도 믿지 않습니다
(5-Factor 인증으로 Zero Trust 구현)

OS 커널에서 함께 검증하는 5-Factor

01	→	02	→	03	→	04	→	05
PID		**세션**		**앱 메타**		**사용자**		**단말**
실행 프로세스		접속 세션		앱 무결성		사용자 인증		기기 인증

5-Factor로 「애플리케이션 신원」을 만들고, 감염 단말의 미인가 프로세스는 격리합니다

출처: 회사 및 기술소개 자료(2026-10)

'스텔스캐슬' 비책③ 성 안에도 격벽을 만듭니다

(앱과 앱 사이만 잇는 방식(App to App)으로 내부를 잘게 나눠 Micro Segmentation 구현)

기존 네트워크 구간 단위
구간 안은 열려 있습니다

- 같은 구간끼리는 서로 통신
- 한 대가 뚫리면 옆으로 확산(Lateral Movement)

→

App to App
승인된 앱끼리만 잇습니다

- 앱↔앱 사이에만 가변 다중 터널
- 수평 이동 차단 · OT 무중단 오버레이

비정상 접근은 Decoy로 유인해 공격행위를 수집해 분석합니다 (Optional)

출처: 회사 및 기술소개 자료(2026-10); 서울시 능동보안 제안서 §3.2(2026-09-11)

'스텔스캐슬'은 설치·사용에 부담이 없습니다

시스템엔 '부하'를 주지 않고 사용자들에겐 '불편'을 더하지 않습니다.

그대로 '오버레이'

기존의 시스템에 그대로 덧씌웁니다

- 서버·방화벽·주소 변경 없음
- 무중단 단계적 적용 — 구간별 실측 후 확대

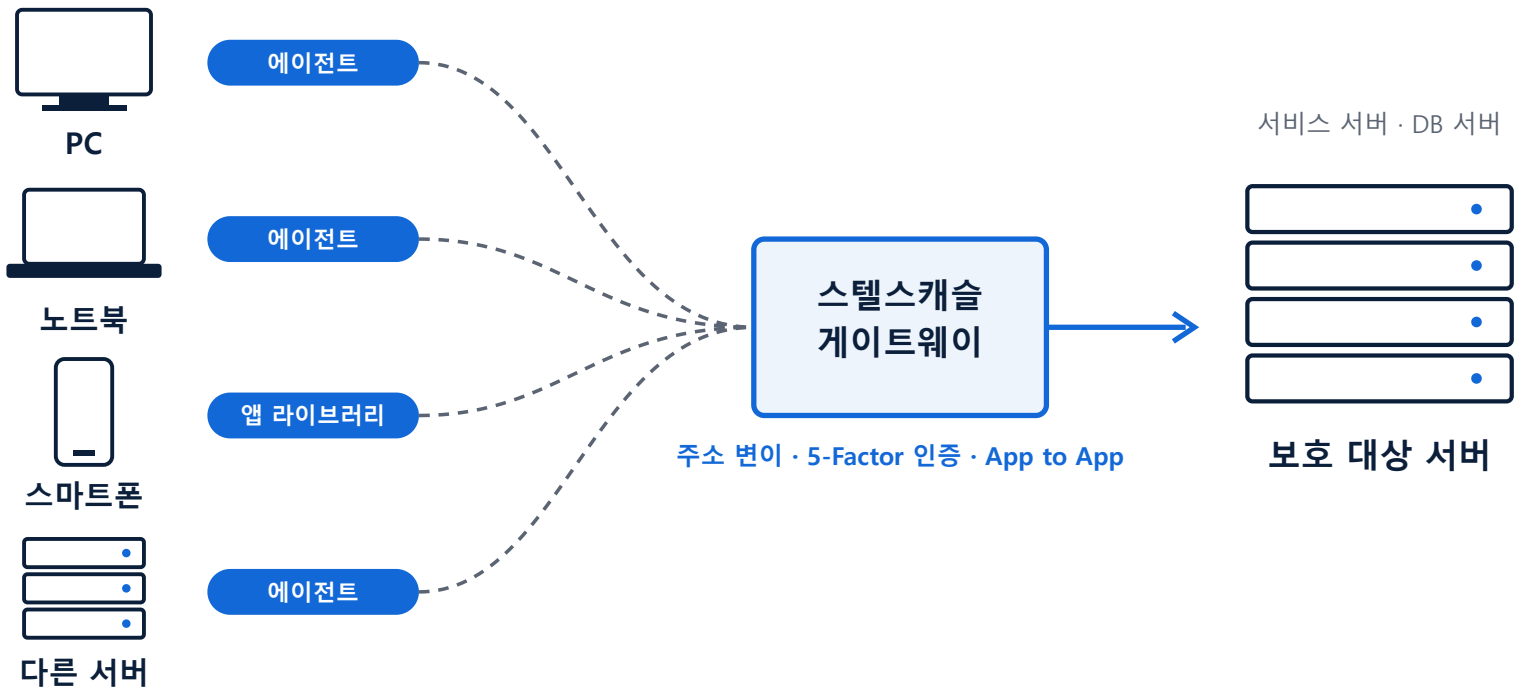
'오버헤드' 거의 없음

시스템 사용자들은 설치 후에도 변화를 느끼지 못합니다

- 40GB 전송 시간 변이 전후 동일(3,634초)
  지연 0%(처리량 기준, KOIST 인증시험 자체점검 결과)
- 서울시 CCTV 실증 — 영상 지연·성능 저하 없음

주: 지연 0%는 처리량 기준 — 접속 수립 지연(p50·p99)은 별도 측정 예정
출처: 회사 및 기술소개 자료(2026-10); 서울시 능동보안 제안서 §4.2(2026-09-11); KOIST 인증시험 자체점검 결과보고서

'스텔스캐슬'(SMTD) 구성도



보호 대상 서버 앞에 '주소 변이 게이트웨이'를 설치하고,
이 서버에 연결하는 단말(PC·노트북·스마트폰·다른 서버)에는 에이전트 또는 앱 라이브러리를 내장해 연결합니다.

(직원 업무망 · 고객 서비스망 · 협력사 네트워크 등 연결 지점 모두에 적용 가능)

'스텔스캐슬' AI 해킹 방어 — "KB국민은행이 실증"

KB국민은행 레드팀, AI(ARTEX) 사용해 화이트 해킹

(2026년 10월 초 '해킹 사건' 직후)

시험

3차

외부망 · 방화벽 개방 · IP 고정

공격 성공

0건

로그상 접속 성공 없음

차수	조건	결과
1차	기존 보안 시스템 + 스텔스캐슬	정찰 실패·공격 성공 0건
2차	기존 보안 해제, 스텔스캐슬만으로 방어	정찰 실패·공격 성공 0건
3차	**IP 고정, Port만 변이해 방어**	**정찰 실패·공격 성공 0건**

출처: 레드팀 침투 시험 경과 보고(2026-10)

"명품 보안" 스텔스캐슬(SMTD)

대한민국 육군·공군·지자체에서 먼저 실증 도입 → 올해 금융·의료·기업으로 확산

2021~22
공군 20전비
영상감시 능동방어

2021~25
육군 사이버전장망
인증서버 능동방어

2023~24
서울시 CCTV 실증
노출 IP·포트 0건

2026
금융(은행·카드)
실증 후 계약 추진 중

의료 (OO대학병원)
포렌식·보안 강화 컨설팅

기업 (A그룹·C상장사 등)
- 제로트러스트 사업
- 고객 개인정보 보호

신기술인증(NET) · 신제품인증(NEP) · GS 1등급

조달 '혁신시제품' (2026.12 지정 예정, 혁신성 · 공공성 평가 완료)

미국 특허 등록(2026.9) · SCI 논문 다수 채택

주: 금융 고객A그룹은 상호 비공개
출처: 회사 및 기술소개 자료(2026-10); 서울시 능동보안 제안서 §4.2(2026-09-11); IR 자료; USPTO 서류(2026-09)

미국의 사이버 보안 비전 "능동방어"

스텔스캐슬 (SMTD)는 '능동방어' 솔루션입니다.

2011

백악관 NSTC

R&D 핵심 주제

2020

NIST 800-53

보안통제 SC-30(3)

2026

NIST 800-172r3

MTD 요건 유지

* 미국은 2010년대부터 '능동방어'를 사이버 보안 비전으로 설정했습니다.
* 메모리 변이 상용화 기업(Morphisec 등)은 있지만
  네트워크 변이를 상용화한 기업은 찾기 어렵습니다.

주: NIST는 선택 통제로 포함
출처: NSTC 2011; NIST SP 800-53r5·800-172r3; morphisec.com

또 하나의 비밀병기 'AEGIS 동형암호' (AEGIS FHE)

양자내성(Quantum Resistant)으로 암호화
암호를 풀지 않고 연산·통계·검색이 이뤄집니다.

01
평문
원본 데이터

→

02
암호화
AGCD 기반 양자내성

→

03
암호문 연산
연산·통계·검색

→

04
결과만 복호화
원본은 노출되지 않음

Privacy-Preserving Data Streaming
연산·통계·검색을 할 때 원본 데이터는 누구에게도 노출되지 않습니다.

출처: 회사 및 기술소개 자료(2026-10)

AEGIS는 '속도'와 '오차' 동형암호의 벽을 넘었습니다.

기존 격자 방식 동형암호
연산 시간이 깁니다

- 10차 연산 0.7997초

→

AEGIS 동형암호
빠르게 연산합니다

- 10차 연산 **0.0075초**
  : 격자 방식보다 100배 이상 빠름
- 자체 측정·제3자 검증 전

AEGIS는 기존의 격자 방식이 아닌 AGCD(근사 최대공약수) 방식 동형암호입니다.

- 격자 방식과 달리 Noise, 다시 말해 오차가 없습니다.
- 격자 방식과 달리 Noise를 제거하는 Bootstrapping도 필요 없습니다.
- 그래서 연산 속도가 근본적으로 빠릅니다.

AEGIS는 금융 · 의료 · 국방 등에서 Privacy-Preserving Data Processing으로 새로운 진보를 가능하게 합니다.

주: 측정 하드웨어·파라미터·보안 수준은 원천 자료에 미기재
출처: 회사 및 기술소개 자료(2026-10)

AI 해킹 방어, "최적의 조합"

「AEGIS로 감싸고, 스텔스캐슬로 숨기고」



공격 표면(외부 접점)은 스텔스캐슬로 숨기고, 데이터는 AEGIS로 감싸서 활용합니다.
내부자가 데이터를 빼내도 무용지물, 황금인 줄 알고 가져가도 보이는 건 모래뿐입니다.

주: 개념 구성 — 적용 구간은 실증에서 정함
출처: 회사 및 기술소개 자료(2026-10)

'검증된 커리어 · 커지는 비전' 연구진·경영진



박유한 대표이사

- 차바이오그룹 전략기획본부장
- KBS비즈니스 대표이사
- KBS 앵커·경제주간
- KBS 워싱턴특파원
- Duke Univ. 펠로우
- 서강대 경제학 석사
- 서울대 경영학과



한희 CSO

- 고려대 정보보호대학원 교수
- 한국국방연구원 실장, ADD 책임연구원
- 국가 과학기술 정책위원
- 국방장관(6명) 과학보좌관
- 국군정보사 여단장
- 모토로라 Lab(T2TRC) 연구소장
- 전자공학박사
- 육군사관학교, 연세대학교, Caltech, Yale 수학



강석진 연구소장

- 서울대 수리과학부 교수
- 과학기술한림원 정회원
- Univ. of Notre Dame 조교수
- UC Berkeley 연구원
- Yale Univ. 박사
- 서울대 수학과



이병도 CTO

- 청주대 디지털보안학과 교수
- 충북과학대 멀티미디어학과 교수
- 사이버리서치 기술이사
- 사이버작전사령부 센터장



김준환 감사

- 세종대 경영전문대학원 초빙교수
- 금융감독원 부원장보
- 금융감독원 은행감독국장
- New York Univ. MBA
- 서울대 경영학과



레드팀 공격 검증

- 전 사이버작전사령부 작전팀장급 인력

주: 직책·약력은 대표 확인(2026-10-11) 기준, 최근 순
출처: 회사 및 기술소개 자료(2026-10); IR 자료

출처

분야	자료
사태·위협	파이낸셜뉴스 2026-10-04·10-07 · 헤럴드경제 10-03 · 머니투데이 10-02 · 뉴데일리 10-08 · ZDNet Korea 10-06 · CrowdStrike 2026 GTR · Anthropic 2025-11-13
글로벌·미국	Zscaler 10-K FY2026 · morphisec.com · NIST SP 800-53r5·800-160 Vol.2·800-172r3 · NSTC 2011
회사 자료	회사 및 기술소개 자료(2026-10) · 금융권 능동보안 제안서(2026-10) · 서울시 능동보안 제안서(2026-09-11) · IR 자료
시험·특허	레드팀 침투 시험 경과 보고(2026-10) · USPTO 서류(2026-09)

출처: 각 장 하단 출처를 분야별로 모음