



트레이드 렌즈

TRADE LENS

투자에 초점을 맞추다.

LENS INSIGHT / No.05

공격·방어·보안산업의 경제성을 읽는 리서치

은행도 뚫렸다

AI 시대, 보안 투자는 어디로 향하나

공격 자동화가 바꾸는 금융보안의
대응 속도와 가치사슬

노출 축소



조치 시간 단축



복구력 확보

더 많은 경보보다 · 안전한 실행 · 지속 가능한 서비스

보안의 가치는 경보의 수가 아니라,
위험이 줄어드는 속도에 있다.

정보 유출·공격 시도·AI 활용의 범위를 구분한다.



01 / RESEARCH VIEW

보안의 가치는 경보가 아니라 조치에서 생긴다

TradeLens 판단 | AI 기능의 수보다 노출·조치·복구를 연결하는 운영 능력에 초점을 맞춘다.

핵심 결론

금융보안의 다음 투자 기준은 알려진 위험이 방치되는 시간을 줄이고, 사고가 나도 핵심 서비스를 유지·복구할 수 있는가다. 기회는 탐지 제품만이 아니라 노출 관리, 접근권한 검증, 대응 연계와 복구 검증에 걸쳐 있다. 다만 필요성이 커졌다고 모든 공급자의 매출·이익이 함께 늘지는 않는다.

핵심 질문	이 보고서의 답
무슨 변화인가	은행권 정보 유출이 이어지는 가운데, AI는 공격과 방어 양쪽의 처리 속도를 바꿀 수 있다. [1] [4]
왜 중요한가	발견이 빨라져도 담당자·승인·수정 배포가 멈추면 위험은 그대로 남는다.
누구에게 가치가 생기나	실제 운영에 연결되고 효과를 입증하는 공급자에게 계약 기회가 생긴다. 비용과 가격이 이익을 가른다.
무엇으로 판단하나	노출 기간, 조치·복구 시간, 정상 거래 오차단, 갱신과 고객별 기여이익을 함께 본다.

위험의 증가와 공급자의 이익은 다른 변수다

보안 투자 증가는 총예산 확대일 수도, 기존 예산의 재배분일 수도 있다. 단발성 긴급 점검이 반복 계약으로 이어지는지, 자동화 절감분이 공급자에게 남는지는 각각 확인해야 한다. 이 보고서는 국내 보안시장 규모나 특정 기업의 신규 수주를 추정하지 않는다.

분석의 기준 단위

경보 한 건이 아니라 위험을 줄인 조치 한 건, 복구된 핵심 서비스 한 단위다. 더 많은 탐지가 더 많은 오탐·승인 대기·운영비를 만든다면 보안성과 사업성과를 모두 다시 평가해야 한다.

분석 기준일 2026.10.03. 국내 사고는 10월 2일 공개 보도와 당국 발표 기준이며, AI의 구체적 역할과 금융거래 피해를 별도로 구분한다.



02 / INCIDENT SCOPE

정보 유출과 금융거래 침해를 같은 말로 쓰지 않는다

2026년 10월 2일 공개 현황. 고객 정보·외주 인력 정보·공격 시도를 나누어 읽는다.

신한·KB국민·하나은행에서는 고객 정보, BNK부산은행에서는 외주 인력 정보의 유출이 보도됐다. 우리·NH농협은행은 당시 파악된 정보 유출 없이 공격 시도를 차단했다고 설명했다. [2] [3]

기관	당시 공개된 대상·규모	범위와 해석
신한은행	고객 약 2만5,000명	대출 관련 개인·신용정보 유출 보도 [3]
KB국민은행	고객 119명	직원용 모바일 업무지원시스템 관련 [2]
하나은행	고객 89명	영업지원시스템 관련 [2]
BNK부산은행	외주 인력 11명	고객 수가 아닌 외주 인력 정보 [2]
우리·NH농협은행	공격 시도	당시 파악된 정보 유출은 없다는 은행 설명 [2]

인원은 보도에 인용된 은행별 집계다. 대상·발표 시점이 다르고 중복 여부가 확인되지 않아 합산하지 않는다. 인원 수로 은행별 보안 수준을 순위화하지 않는다.

은행 설명의 적용 범위

KB국민·하나은행은 관련 시스템이 고객의 인터넷·모바일뱅킹 거래 채널과 구분된다고 설명했다. [2] 개인정보 유출은 중대한 사고지만, 그 사실만으로 예금 탈취나 핵심 계정계의 침해까지 입증되는 것은 아니다.

투자 논의의 출발점은 ‘전체 노출 자산’이다

금융위원회는 10월 2일 긴급회의에서 외부에 노출된 IT 시스템·서비스 점검과 위협정보 공유를 강조했다. [1] TradeLens는 이를 주력 거래 채널뿐 아니라 업무지원·외부 연계까지 자산과 권한의 관리 범위를 넓혀야 하는 문제로 해석한다.

읽어야 할 변화

사고 건수만 세기보다 어떤 업무와 데이터가 외부에서 접근 가능했는지, 담당자·통제·조치가 연결돼 있었는지를 본다. 현재 공개 범위를 넘어 모든 사고의 원인이 같다고 가정하지 않는다.



03 / AI & ATTRIBUTION

AI는 공격을 가속할 수 있다. 사고 원인을 대신 설명하지는 않는다

AI 활용 현황, 기술적 가능성, 개별 사고의 인과관계를 분리한다.

영국 NCSC와 협력 기관의 2026년 6월 공동 성명은 AI가 취약점 발견과 악용 사이의 시간을 줄일 수 있으며, 방어에도 활용될 수 있다고 평가했다. [4] 이는 위협 환경에 대한 기관의 판단이지 이번 국내 사고가 모두 무인 자율 공격이었다는 증거는 아니다.

구분	뜻	보고서에서의 경계
AI 보조	분석·분류·코드 이해 등 일부 작업에 모델 활용	AI 사용만으로 전체 공격의 자율성을 판단하지 않음
공격 자동화	반복 시도와 작업 연결을 소프트웨어로 수행	일반 스크립트 자동화와 AI 활용은 동일하지 않음
자율 공격	목표 해석·실행·조정을 폭넓게 시스템에 위임	사건별 도구·로그·사람의 개입 범위 등 근거가 필요

BNK부산은행의 AI 에이전트 활용 공격 설명도 보도에 인용된 은행 측 설명의 범위로 읽는다. [2] 이를 다른 은행의 모든 사고에 확대하거나 모델의 성능을 정량화하는 근거로 쓰지 않는다. 반대로 구체적 AI 기여도가 확정되지 않았다는 이유로 노출 자산과 권한 점검을 미룰 필요도 없다.

TradeLens 분석 | 변하는 것은 반복 작업의 경제성이다

시도 한 번의 비용이 낮아지고 반복이 쉬워질수록, 오랫동안 남아 있는 작은 취약점도 관리 부담이 된다. 따라서 공급자의 차별성은 “AI로 탐지”라는 설명보다 취약점을 닫는 업무와 연결되는가에 있다. 이 관계는 분석 가설이며 국내 사고의 AI 기여율 추정이 아니다.

양방향 자동화를 함께 본다

AI가 방어의 분류·우선순위 판단도 개선하면 같은 예산으로 더 넓은 범위를 관리할 수 있다. 보안 수요의 확대와 단위 서비스 가격 하락이 동시에 발생할 가능성이 공급자 이익을 가르는 변수다.

04 / EMPIRICAL EVIDENCE

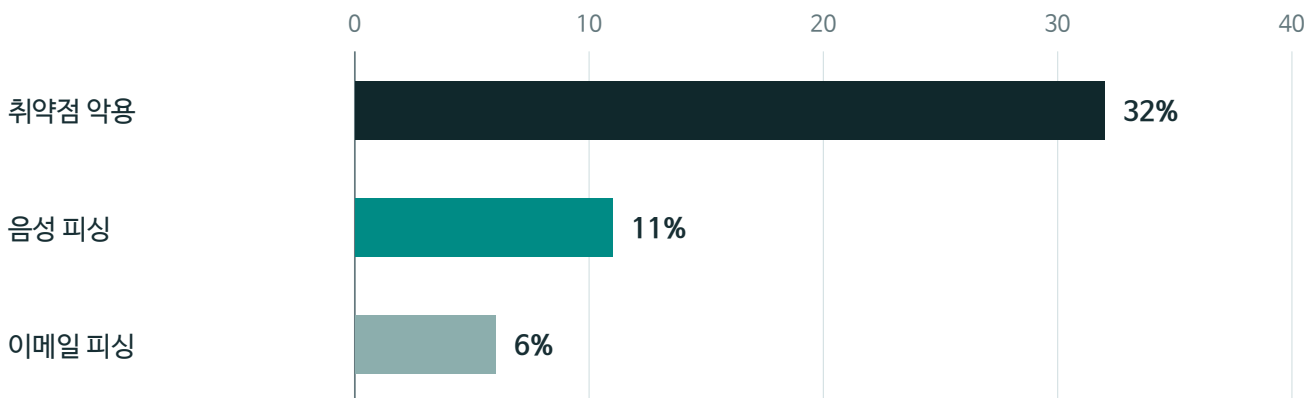
새로운 AI 위협 앞에서도 기본 통제가 중요하다

Mandiant의 2025년 사고조사 표본을 읽는다. 한국 은행의 현재 침해 확률이 아니다.

M-Trends 2026은 2025년 수행한 표적 공격 조사에서 최초 침투 경로로 취약점 악용 32%, 음성 피싱 11%, 이메일 피싱 6%를 제시했다. 아래는 같은 조사 범위의 일부 경로만 비교한 것이다. [5]

최초 침투 경로 · 선택 항목

조사 사례 내 비중 · %



출처: Mandiant M-Trends 2026, Executive Edition 3쪽. 관측 기간 2025.01 - 12. 선택 항목이므로 합계가 100%인 전체 구성표가 아니다. [5]

관찰	TradeLens가 연결하는 방어 과제
취약점 악용	노출된 자산 목록, 수정 우선순위, 실제 배포 완료 여부를 연결한다.
음성 기반 사회공학	신원 확인·업무 승인·권한 변경 절차가 기술 탐지를 보완해야 한다.
이메일 기반 사회공학	메일 통제와 계정·단말의 사후 이상행위 확인을 분리하지 않는다.

통계가 말하지 않는 것

이 표본은 전 세계 모든 조직을 대표하는 전수 통계가 아니다. 시가 사용된 공격의 비중도, 국내 은행의 사고 원인 비중도 아니다. 숫자는 여러 방어 층이 필요한 이유를 보완하며 특정 제품의 효과나 시장점유율을 입증하지 않는다.



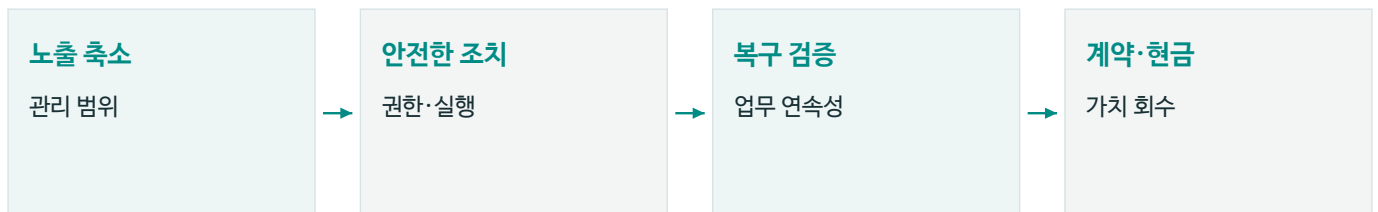
05 / SECURITY VALUE CHAIN

보안 예산의 목적지는 ‘연결된 통제’다

단일 제품 대체론보다 노출 축소·접근권한·대응·복구의 연결을 본다.

NIST는 탐지·대응·복구를 조직의 위험관리와 연결하고, 바젤위원회는 핵심 업무의 의존관계와 제3자 관리를 운영복원력의 일부로 다룬다. [6] [8] 다음 표는 이를 사업 기회와 성과 측정에 연결한 TradeLens의 분석 틀이다.

투자 영역	실제 산출물	성과를 확인할 지표
노출 자산·취약점 관리	소유자가 정해진 자산 목록, 위험별 조치	미관리 자산, 미조치 고위험 항목의 기간
신원·권한·API 통제	필요한 사람·단말·데이터에 한정된 접근	과도한 권한, 권한 검증 테스트, 오차단
탐지·관제·대응 연계	근거가 있는 경보에서 승인된 조치까지	확인·격리 시간, 수작업 대기, 재발
복구·업무 연속성	데이터와 의존 서비스까지 검증한 복구	복구 소요시간, 데이터 정합성, 실제 업무 시험



개념적 가치 연결. 영역별 예산 비중이나 국내 금융회사의 실제 발주 순서를 뜻하지 않는다.

‘장비보다 운영’은 장비가 불필요하다는 뜻이 아니다

장비를 줄여야 한다는 결론이 아니다. 이미 있는 제품이 서로 다른 데이터·권한·책임 체계에 갇혀 있다면 연계·운영·검증이 우선일 수 있다. 신규 제품과 운영 통합 중 무엇이 더 큰 위험 감소를 주는지는 현재 자산과 병목에 따라 달라진다.

가치귀속의 조건

플랫폼, 구축 사업자, 관제 서비스, 복구 전문업체가 서로 다른 역할을 맡을 수 있다. 넓은 공급 범위는 매출 기회와 함께 연계 비용·책임·서비스 부담도 늘린다. 계약 범위와 비용 구조를 함께 읽는다.



06 / RESPONSE-TIME LAB

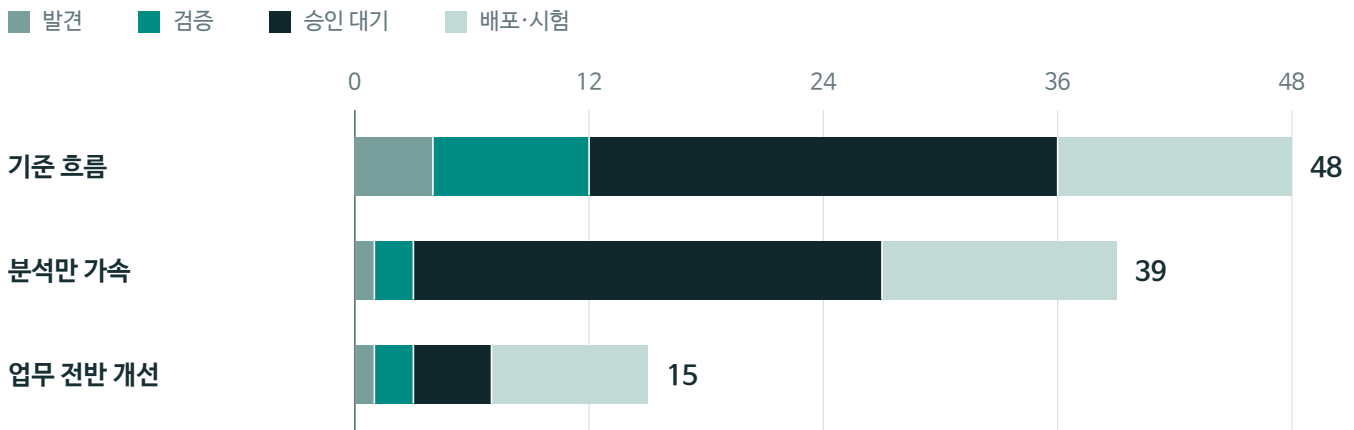
분석이 빨라져도 조치가 48시간에서 39시간에 그칠 수 있다

설명용 가정 | 부분 자동화와 전체 업무 흐름 개선을 같은 시간 기준에서 비교한다.

모형 A | 한 건의 취약점 조치에 걸리는 경과시간

기준 흐름은 발견 4시간 + 검증 8시간 + 승인 대기 24시간 + 배포·시험 12시간 = 48시간이다. 단계가 순서대로 진행되고 중복되지 않는다고 가정한다. 실제 은행의 측정치·인력시간·계약상 목표가 아니다.

단위: 시간 · 설명용 가정



가정 시나리오	발견 / 검증 / 승인 / 배포	총시간	기준 대비 단축
기준 흐름	4 / 8 / 24 / 12시간	48시간	—
분석 단계만 가속	1 / 2 / 24 / 12시간	39시간	18.8%
업무 전반 개선	1 / 2 / 4 / 8시간	15시간	68.8%

계산: $(48-39) \div 48=18.75\%$, $(48-15) \div 48=68.75\%$. 그림은 단계별 경과시간의 누적이며 병렬 작업·재시도·재발은 미반영이다.

이 계산이 바꾸는 구매 기준

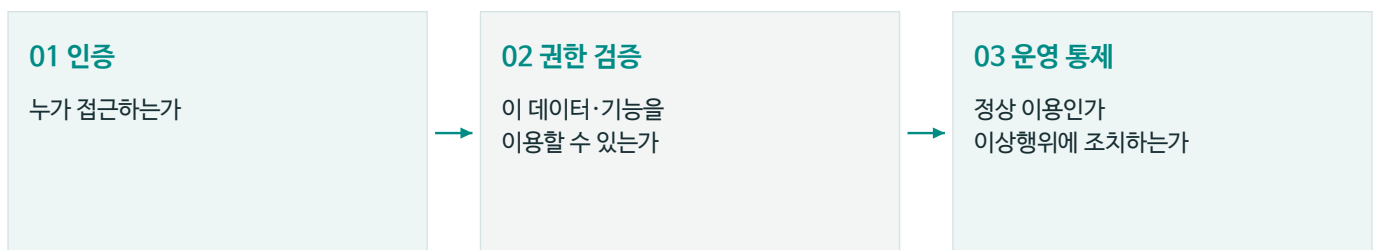
AI 분석 시간만 줄이는 기능과 담당자 배정·권한·승인·안전한 배포까지 바꾸는 서비스는 경제적 효과가 다르다. 승인 단축은 통제를 없애는 것이 아니라 사전 정의된 권한과 검증된 절차를 통해 이루어져야 한다.

07 / IDENTITY & API CONTROL

로그인 성공은 모든 데이터의 열람 허가가 아니다

네트워크 접근, 사용자 인증, 개별 데이터 권한은 서로 다른 통제다.

OWASP의 API 보안 원칙은 개별 데이터 객체에 접근하는 기능에서 권한을 확인해야 한다고 설명한다. [7] 따라서 “인증된 사용자”라는 사실과 “이 기록을 읽거나 바꿀 권한”은 구분된다. 아래는 일반적 통제 구조이며 이번 은행 사고의 특정 원인을 재구성한 것이 아니다.



통제 층	답해야 하는 질문	다른 통제가 대신하지 못하는 부분
사용자·단말 확인	누가, 어떤 단말로 접근하는가	확인된 사용자에게 허용할 데이터 범위는 별도
업무·데이터 권한	이 사람이 이 기록·기능을 사용할 수 있는가	네트워크 접속 허용과 개별 데이터 권한은 별도
행위·운영 확인	허용된 접근도 비정상적으로 이용되는가	사후 탐지로 코드의 권한 검증을 대신할 수 없음

제품 경계보다 데이터의 경계를 따라간다

웹·API 보호, 신원·단말 통제와 애플리케이션의 권한 검증은 보완 관계다. 금융회사가 구입할 것은 하나의 명칭이 아니라 외부·지원 시스템까지 작동하는 통제 조합이다. 도입 전후의 권한 테스트와 정상 사용자 오차단을 함께 확인해야 한다.

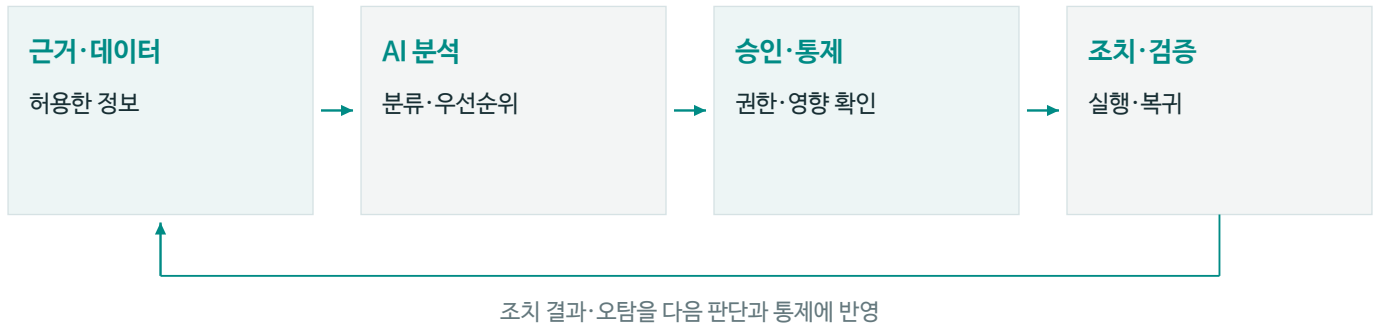
사업적 의미

권한 체계를 업무에 맞게 설계하고 기존 시스템에 적용·시험하는 작업은 제품 판매와 다른 비용 구조를 갖는다. 구축 완료와 반복 운영의 계약·책임을 구분할 때 지속적인 서비스 가치도 더 명확해진다.

08 / AI IN DEFENSE

방어용 AI의 성능은 안전하게 실행될 때 의미가 있다

자동 조치 범위를 정하지 않은 자동화는 새로운 운영 위험을 만들 수 있다.



TradeLens의 방어 운영 설계도. NIST의 탐지·대응·복구 및 조직 역할 구분을 바탕으로 재구성했다. 기관의 인증이나 특정 제품 구조가 아니다. [6]

설계 항목	실행 전에 확인할 것
데이터와 근거	어떤 로그·정보를 모델에 주는가. 판단의 원문 근거를 남길 수 있는가.
조치 권한	읽기·분석과 계정 차단·시스템 변경을 분리한다. 영향이 큰 조치는 승인 범위를 명시한다.
안전 장치	오차단 검증, 변경 이력, 되돌리기와 수동 전환 절차를 갖춘다.
성능 평가	탐지율만이 아니라 미탐·오탐·정상 거래 영향·전체 조치 시간을 함께 본다.

제도 발표와 매출 인식 사이에는 실행 조건이 있다

금융위원회는 2026년 5월 보안 목적 AI 활용을 위한 망분리 규제의 조건부 완화 추진을 발표했다. [10] 이는 모든 금융회사에 대한 일괄 허용이나 실제 구매 완료를 뜻하지 않는다. 도입 가능성은 적용 조건, 데이터 처리, 배포 방식과 기관별 절차까지 연결해 보아야 한다.

공급자의 실질적 차별성

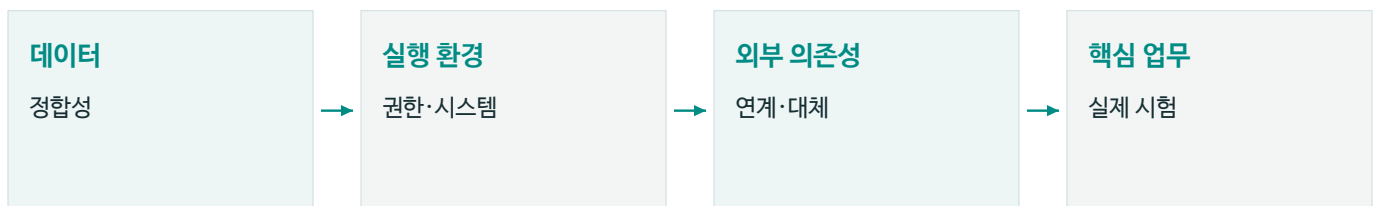
모델 점수만 높아서 부족하다. 고객의 배포·데이터 조건을 충족하고, 권한이 제한된 상태에서도 업무에 연결되며, 오작동 때 복귀할 수 있어야 한다. 이 실행 비용을 가격과 계약에 반영하는 능력이 중요하다.

09 / RESILIENCE & THIRD PARTIES

막는 능력과 다시 운영하는 능력을 함께 산다

복원력은 백업 보유 여부가 아니라 핵심 업무를 이어갈 수 있는 능력이다.

FSB의 2026년 8월 발표는 고성능 AI의 사이버 위협과 관련해 금융회사의 대응·복구와 핵심 제3자 서비스의 복원력을 강조했다. [9] 바젤위원회 원칙도 핵심 업무를 제공하는 내부·외부 의존관계의 파악과 제3자 관리에 초점을 둔다. [8]



함께 복구할 것	검증해야 하는 결과
데이터와 거래 상태	백업이 존재하는가를 넘어 필요한 시점의 데이터 정합성이 맞는가
계정·권한·실행 환경	복구 후 필요한 인력과 서비스만 안전하게 접근·실행할 수 있는가
외부 서비스·연계	핵심 외부 제공자 장애 시 대체·전환·연락 체계가 작동하는가
고객이 쓰는 핵심 업무	실제 업무 시험에서 처리와 통제가 함께 정상화되는가

외부 위탁이 위협의 소멸을 뜻하지는 않는다

공통 서비스가 효율과 가시성을 높일 수 있지만 의존성이 집중될 수도 있다. 공급자를 늘리는 것만으로 복원력이 생기는 것도 아니다. 상호 의존관계와 전환 가능성을 시험하고 책임·대응 창구를 정해야 한다. 이는 국내 은행의 특정 위탁 구조나 사고 원인을 추정한 것이 아니다.

경제적 해석

복구·훈련·연계 점검은 정기 서비스 기회를 만들 수 있다. 다만 무제한 대응 의무나 모호한 복구 책임을 떠안으면 매출 증가가 인건비·배상·대기 비용으로 상쇄될 수 있다. 서비스 수준과 책임 범위의 가격을 함께 본다.



10 / SUPPLIER ECONOMICS

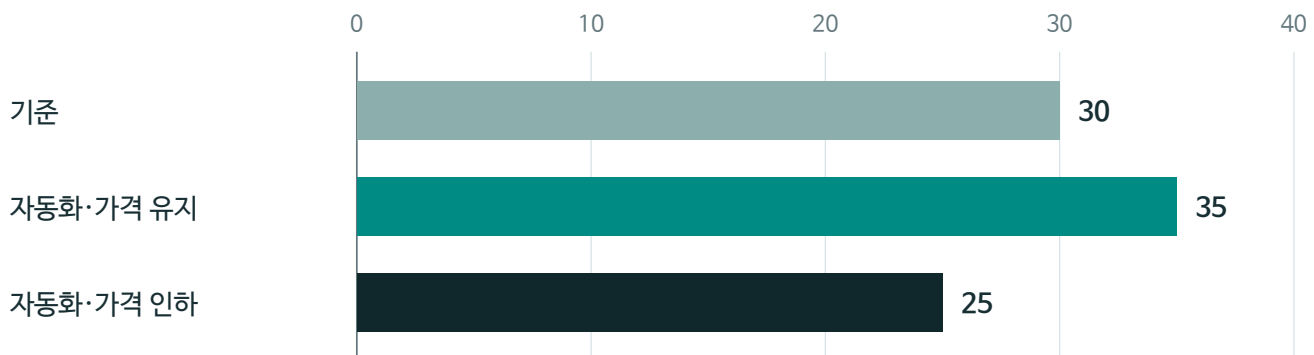
자동화해도 서비스 가격이 더 내려가면 이익은 줄어든다

설명용 가정 | 같은 고객의 연간 계약에서 가격과 직접 제공비용을 분리한다.

연간 가정 · 백만원	기준	자동화·가격 유지	자동화·가격 인하
계약 매출	100	100	90
직접 연산·도구비	10	20	20
직접 운영 인건비	40	25	25
직접 고객지원비	20	20	20
직접 제공비용 합계	70	65	65
고객별 기여이익	30	35	25

고객별 기여이익 비교

백만원/년 · 설명용 가정



기여이익 = 계약 매출 - 해당 고객에 직접 귀속한 제공비용. 전사 연구개발·공통 관리·영업비·세금 등을 차감한 순이익이 아니다. 특정 기업의 요금·원가·마진 추정 이 아니다.

절감된 시간이 누구의 이익이 되는가

자동화로 연산·도구비가 10 늘고 인건비가 15 줄면 직접비는 5 감소한다. 그러나 가격이 10 내려가면 기여이익은 30에서 25로 줄어든다. 또한 작업시간 절감은 인력 재배치나 추가 고객 수용으로 이어질 수 있으며 즉시 현금 인건비 절감이 되는 것은 아니다.

확인할 사업 지표

유료 배포·갱신은 수요의 증거이고, 고객당 연산비·운영시간·지원비는 수익성의 증거다. 유지 가격, 도입 비용 회수와 수급 까지 이어져야 반복 계약이 지속 가능한 현금흐름이 된다.



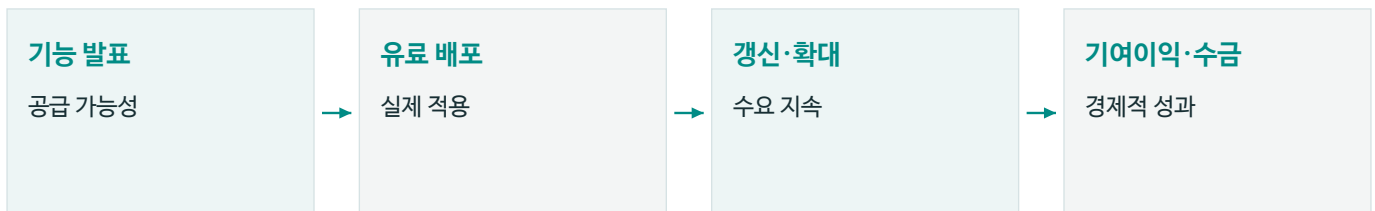
11 / KOREAN SUPPLIER MAP

‘시 보안주’라는 이름 대신 공급 범위를 읽는다

회사 공식 제품 설명을 사업 노출의 사례로 사용한다. 사고 관련 수주나 납품 관계를 뜻하지 않는다.

기업·제품	공식 설명에 나타난 범위	사업성으로 연결해 볼 항목
안랩 AhnLab XDR [11]	탐지·대응 연계, 노출 관리와 AI 분석	기존 고객 확장, 데이터 연계 범위, 운영·지원 비용
이글루코퍼레이션 SPiDER SOAR [12]	플레이북 기반 대응 자동화와 이기종 연계	실제 자동 조치 범위, 구축과 반복 운영의 계약 구분
지니언스 Genian ZTNA [13]	사용자·단말 맥락에 따른 네트워크 접근 통제	적용 자산과 갱신, 정책 운영 부담; API 개별 권한은 별도
펜타시큐리티 WAPPLES [14]	웹 애플리케이션·API 보호	적용 서비스·정상 요청 오차단·유지 서비스의 계약 범위

상장 여부와 무관한 산업 사례이며 순위·종목 추천이 아니다. 회사 자료는 제품 기능의 설명이지 금융권 실제 도입률이나 수익성의 독립 검증 자료가 아니다.



같은 수요 변화가 같은 손익을 만들지는 않는다

같은 보안 테마라도 라이선스, 구독, 구축·통합, 상주·원격 관제의 매출 인식과 원가 구조는 다르다. 특정 은행의 사고를 이들 기업의 매출로 바로 환산할 수 없다. 신규 기능 공개 역시 유료 고객·갱신·현금 회수와 구분해야 한다.

TradeLens가 선별하는 것은 주가가 아니라 사업 구조다

반복 계약의 비중만 높다고 좋은 사업은 아니다. 가격 유지, 연산·인력 비용 통제, 과도한 맞춤 구축의 감소와 명확한 책임 범위가 함께 필요하다. 공개되지 않은 수주·고객·마진을 채워 넣지 않는다.



12 / OUTLOOK & MONITORING

투자의 방향은 위험이 줄어드는 속도로 확인한다

기본 판단은 선택적 확대·재배분이다. 전체 시장의 매출 증가율이나 기업별 수혜를 예측하지 않는다.

확인할 영역	판단을 강화하는 증거	판단을 약화시키는 증거
수요의 실현	예산 승인→유료 배포→반복 갱신	긴급 진단 뒤 추가 도입이 끊김
보안 운영	노출 기간·조치 대기 감소, 오차단 관리	경보만 증가하고 실제 조치가 정체
복구와 의존성	핵심 업무·제3자 연계 복구 시험 통과	백업 보유에도 실제 서비스 복구 실패
공급자 경제성	가격·직접비·지원비가 기여이익을 지지	가격 인하와 연산·인력 비용 증가의 중첩

기본 경로 | 새 기능보다 통제의 연결에 선택적 투자

외부 자산 점검에서 시작한 요구가 권한·대응·복구의 상시 운영으로 이어지면 반복 서비스 기회가 넓어진다. 반대로 단발성 대응에 머물거나 예산이 재배분될 뿐이면 모든 공급자에게 추가 매출이 생기지 않는다.

반증 조건 | 기술 성능 향상만으로 결론을 유지하지 않는다

AI가 방어 작업도 더 효율적으로 만들고 경쟁이 절감분을 가격에 반영하면, 금융회사는 더 나은 보안을 얻어도 공급자 수익성은 약해질 수 있다. 오탐·오차단이 늘어 수동 검토와 고객지원이 다시 증가하는 경우도 자동화의 경제성을 약화시킨다.

최종 판단

은행권 사고는 보안의 필요성을 보여주지만, 보안산업의 이익을 보장하지 않는다. AI 시대의 투자 기준은 위험의 발견에서 안전한 조치·복구까지 이어지는 능력이다. 그 효과를 검증 가능한 계약과 지속 가능한 제공비용으로 바꾸는 곳에 경제적 가치가 남는다.

사고 원인과 범위의 후속 발표는 사건 해석을 바꿀 수 있다. 본 보고서의 수치 모형은 실제 사고·회사 전망이 아니며 모든 제도·회사 설명에는 각 발표 시점의 범위를 적용한다.



13 / SOURCE REGISTER

사건·기술 원칙의 근거를 원문으로 연결한다

본문의 청록색 출처번호와 아래 자료명·‘원문 열기’를 누르면 원문으로 이동한다.

01. 금융위원회 | 최근 발생하는 금융권 침해위험에 면밀히 대응해 나가겠습니다

원문 열기

2026.10.02 · 공식 보도참고 · 긴급회의, 외부 노출 시스템 점검·정보 공유

02. YTN | 국민·하나·부산은행도 정보 유출…우리·농협은 접근 시도 차단

원문 열기

2026.10.02 · 보도 · 은행 설명을 인용한 유출 대상·규모·시스템 구분

03. 이코노미스트 | “내 정보도?” 신한·KB이여 하나은행도 뚫렸다…고객정보 유출

원문 열기

2026.10.02 · 보도 · 신한 약 2만5천명 등 은행별 공개 현황

04. 영국 NCSC 외 사이버보안기관 | The AI shift in cyber risk: why leaders must act now

원문 열기

2026.06.22 · 공동 성명 · AI와 공격·방어 속도, 기본 통제·대응 준비

05. Google Cloud · Mandiant | M-Trends 2026 — Executive Edition

원문 열기

2026.03 · 1차 사고조사 자료 · PDF 3쪽, 2025년 조사 사례의 최초 침투 경로

06. 미국 NIST | SP 800-61r3: Incident Response Recommendations and Considerations

원문 열기

2025.04 · 공식 지침 · 본문 5 - 9쪽, 탐지·대응·복구와 조직의 역할

07. OWASP | API1:2023 — Broken Object Level Authorization

원문 열기

2023 · 기술 원문 · 개별 데이터·기능의 접근권한 검증

복원력·제도·기업 설명의 범위를 구분한다

08. 바젤은행감독위원회 · BIS | Principles for Operational Resilience

원문 열기

2021.03 · 공식 원칙 · 본문 6 - 7쪽, 의존관계·제3자·사고 대응

09. 금융안정위원회 FSB | FSB Chair warns of risks arising from frontier AI models

원문 열기

2026.08.31 · 공식 발표 · 의장 견해, 금융회사 대응·복구·핵심 제3자 복원력

10. 금융위원회 | 금융권 AI 전환 본격화! 금융분야 망분리 규제 완화

원문 열기

2026.05.26 · 공식 발표 · 5월 22일 간담회, 보안 목적 AI 활용의 조건부 추진

11. 안랩 | AhnLab XDR, 더 넓어진 가시성과 AI로 보안 운영의 효율을 높인다

원문 열기

2026.08.26 · 회사 설명 · XDR, 노출 관리, AI 분석의 제품 범위

12. 이글루코퍼레이션 | SPiDER SOAR

원문 열기

2026.10.03 기준 · 공식 제품 설명 · 플레이북·이기중 솔루션 연계·대응 자동화

13. 지니언스 | Genian ZTNA

원문 열기

2026.10.03 기준 · 공식 제품 설명 · 사용자·단말 맥락에 따른 네트워크 접근

14. 펜타시큐리티 | WAPPLES

원문 열기

2026.10.03 기준 · 공식 제품 설명 · 웹 애플리케이션·API 보호 범위

자료 적용: 은행별 사건은 당시 보도·은행 설명, 당국 대응은 공식 발표를 기준으로 구분한다. 해외 사고조사 표본과 국내 사고를 합산하거나 AI의 인과 효과로 해석하지 않는다.



작성 기준·면책고지·이용 안내

확인된 사건, 기관·회사 설명, TradeLens의 판단과 설명용 계산을 구분한다.

항목	적용 기준
시점·사건	분석 기준일 2026.10.03. 국내 사고 현황은 10월 2일 공개 보도·은행 설명 기준이며 후속 조사로 달라질 수 있다.
표본·자료 성격	Mandiant 수치는 2025년 조사 사례. AI 인과 효과나 한국 전체 금융기관의 침해 확률이 아니다. 기관·회사 설명은 각 발표일 범위로 사용한다.
모형 A · 7쪽	단계별 경과시간의 순차 합계. 병렬 작업·재시도 등은 제외한다. 인력시간이나 실제 은행 조치 수준을 측정하지 않는다.
모형 B · 11쪽	연간 계약·직접 연산비·인건비·지원비의 가정. 기여이익은 공통비·세금 전이며 특정 업체 전망이 아니다.
제공 범위	금융보안의 산업구조·운영·사업 경제성 분석. 매매 의견·시점·목표주가·적정주가 및 개인별 투자자문은 제공하지 않는다.

도식과 차트는 TradeLens가 재구성했으며 원기관의 승인·보증을 뜻하지 않는다. 반올림은 계산 후 표시 단계에서 적용한다. 본 보고서는 시스템에 대한 침투시험·안전성 인증 자료가 아니다.

면책고지

본 보고서는 기술·산업 및 기업의 사업구조·성장성·수익성에 관한 일반적인 정보 제공을 목적으로 합니다. 매수·매도 의견·시점, 적정주가·목표주가 및 이용자별 투자자문은 제공하지 않습니다. 수록 정보와 분석은 작성일 기준이며 정확성·완전성·최신성을 보장하지 않습니다. 전망·추정 및 예시 계산에는 불확실성이 있으며, 원금이나 투자수익을 보장하지 않습니다.

투자판단은 이용자의 책임으로 이루어져야 합니다. 관계 법령상 책임이 인정되는 경우를 제외하고, 트레이드렌즈는 본 보고서 이용에 따른 투자손실에 책임을 지지 않습니다.

저작권 및 이용 제한

본 보고서의 서술·도표·디자인·편집 및 구성 중 트레이드렌즈가 권리를 보유한 부분은 관계 법령에 따라 보호됩니다. 개인 열람·보관 외에 사전 서면 동의 없이 전부 또는 일부를 수정·편집·번역·재가공하거나 복제·전송·재게시·재배포·판매할 수 없습니다. 유료·무료 제공 및 파일·화면 캡처 등 형태를 불문하며, 로고·출처·권리표시를 제거하거나 제3자 명의로 배포하는 행위도 금지합니다.

다만 관계 법령상 허용되는 이용과 제3자 자료의 개별 이용허락조건은 그에 따릅니다. 공유는 트레이드렌즈 공식 게시페이지의 원문 링크를 이용해 주시기 바랍니다.