



트레이드 렌즈
TRADE LENS

Bringing investing into focus.

LENS INSIGHT / No.05

Reading the economics of attacks, defense and security suppliers

Banks Breached

Where Does Security Investment Go in the AI Era?

How attack automation reshapes response speed and value capture in financial cybersecurity

Reduce exposure



Shorten response



Validate recovery

Beyond alert volume · safe execution · sustainable service economics

**Security value is not the number of alerts.
It is the speed at which risk is reduced.**

Distinguishing data leaks, attempted intrusions and AI attribution.

01 / RESEARCH VIEW

Security creates value when alerts become action

TradeLens view | Focus on the operating link between exposure, response and recovery—not the number of AI features.

Core conclusion

The next test for financial cybersecurity investment is whether it **shortens the time that known risk remains unresolved and keeps critical services recoverable**. Opportunities span exposure management, authorization, response integration and recovery validation. Greater need does not mean higher revenue or profit for every supplier.

Core question	This report's answer
What is changing?	Bank data leaks coincide with AI's potential to accelerate both attack and defense. [1] [4]
Why does it matter?	Faster discovery leaves risk unresolved when ownership, approval or deployment stalls.
Who may capture value?	Suppliers that integrate into operations and demonstrate results. Price and delivery cost determine profit.
What should be measured?	Exposure duration, response/recovery time, legitimate activity blocked, renewals and customer contribution.

Threat growth and supplier profit are different variables

Spending can expand in total or move between existing categories. An emergency assessment must still become a recurring contract, and automation savings need not remain with the supplier. This report does not estimate Korea's security-market size or undisclosed vendor orders.

The unit of analysis

An action that reduces risk and a critical service restored—not an alert generated. More detection can also mean more false positives, approval queues and operating expense. Both security outcomes and commercial outcomes must be tested.

Analysis date: 3 October 2026. The domestic incident snapshot uses 2 October reports and official announcements. AI attribution and financial-transaction harm are treated separately.

02 / INCIDENT SCOPE

A data leak does not prove a transaction breach

Publicly reported position on 2 October 2026. Distinguish customers, contractors and attempted intrusions.

Customer information leaks were reported at Shinhan, KB Kookmin and Hana; contractor information was exposed at BNK Busan. Woori and NH NongHyup said attempts had been blocked with no information leakage identified at that point. [2] [3]

Institution	Reported people affected	Scope and interpretation
Shinhan	About 25,000 customers	Loan-related personal/credit data [3]
KB Kookmin	119 customers	Employee mobile work-support system [2]
Hana	89 customers	Sales-support system [2]
BNK Busan	11 contractors	Contractor information—not customer count [2]
Woori / NH NongHyup	Attempted intrusions	Banks said no leakage had been identified then [2]

Counts are bank-level figures cited in reporting. Different populations, disclosure times and unknown overlap prevent aggregation. They do not rank the banks' security quality.

What the banks' statements cover

KB Kookmin and Hana described the affected systems as separate from customer internet/mobile banking transaction channels. [2] **Personal-data exposure is serious, but does not by itself establish stolen deposits or compromise of core banking.**

Begin the investment discussion with the full exposed estate

At its 2 October emergency meeting, the FSC stressed checks of externally exposed IT systems/services and threat-information sharing. [1] TradeLens reads this as a need to manage assets and permissions across support and external-facing services—not only the principal transaction channel.

What to look for

Beyond incident counts, ask which work and data were reachable, who owned them, and whether controls led to action. Public disclosures do not establish one common root cause for every incident.

AI can accelerate an attack. It does not explain every breach.

Separate reported AI use, technical possibility and causation in an individual incident.

In June 2026, the NCSC and partner agencies assessed that AI can compress the gap between vulnerability discovery and exploitation, while also supporting defense. [4] That assessment does not prove that every recent Korean incident was an autonomous attack without human involvement.

Category	Meaning	Interpretive boundary
AI assistance	Models support analysis, classification or understanding code	AI use alone does not establish end-to-end autonomy
Attack automation	Software repeats attempts and connects tasks	Conventional scripts are not evidence of AI use
Autonomous attack	A system takes on broad planning, execution and adjustment	Attribution requires incident-specific evidence on tools, logs and human involvement

BNK Busan's description of an AI-agent-enabled attack is treated as a bank statement cited in reporting. [2] It is not extrapolated to every other bank or used to quantify model capabilities. Unresolved AI attribution is also no reason to postpone exposed-asset and permission checks.

TradeLens analysis | The economics of repetition may change

When each attempt costs less and repetition becomes easier, small weaknesses left unresolved for long periods can become more consequential. Supplier differentiation lies in **connecting detection to remediation**, not merely labeling it AI. This is an analytical hypothesis, not an estimate of AI's share of the Korean breaches.

Account for automation on both sides

If AI also improves defensive triage and prioritization, the same budget may cover more assets. Growing demand can coexist with lower service prices. That combination matters for suppliers' profit.

04 / EMPIRICAL EVIDENCE

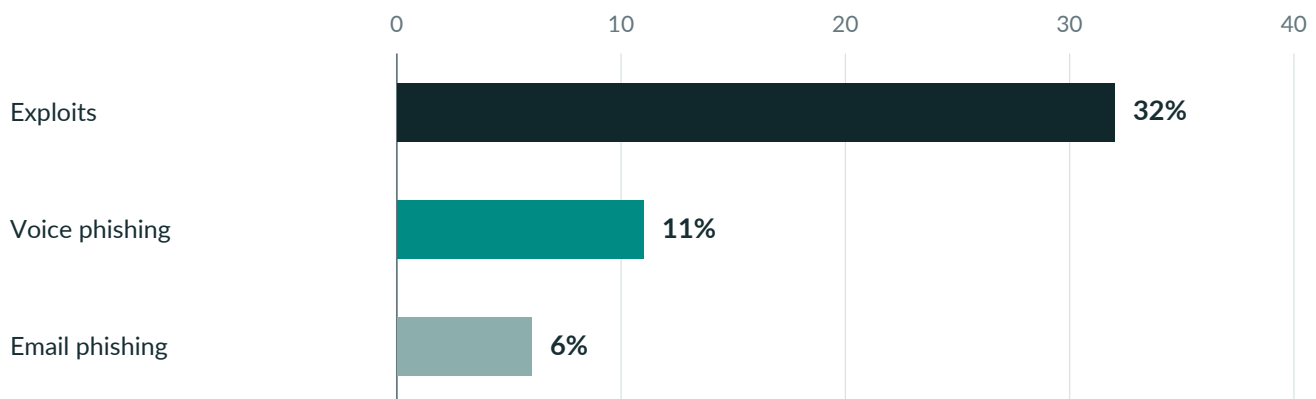
AI-era attacks still test baseline controls

Mandiant's 2025 investigation sample is not a current breach probability for Korean banks.

M-Trends 2026 reports exploits at 32%, voice phishing at 11% and email phishing at 6% of initial infection vectors in its 2025 investigations. The chart compares selected vectors within that same scope. [\[5\]](#)

Selected initial infection vectors

Share within investigations · %



Source: Mandiant M-Trends 2026, Executive Edition, p.3. Investigations: 1 January–31 December 2025. Selected categories—not a complete distribution summing to 100%. [\[5\]](#)

Observation	Defensive task in TradeLens's framework
Exploitation	Connect exposed-asset ownership, remediation priority and completed deployment.
Voice-based social engineering	Identity checks, approvals and permission-change procedures complement technical detection.
Email-based social engineering	Connect email controls with subsequent account and endpoint behavior.

What the statistics do not show

This is not a census of all organizations. It is neither the share of attacks using AI nor the root-cause mix of Korean bank incidents. The data supports a layered approach; it does not establish a product's efficacy or market share.

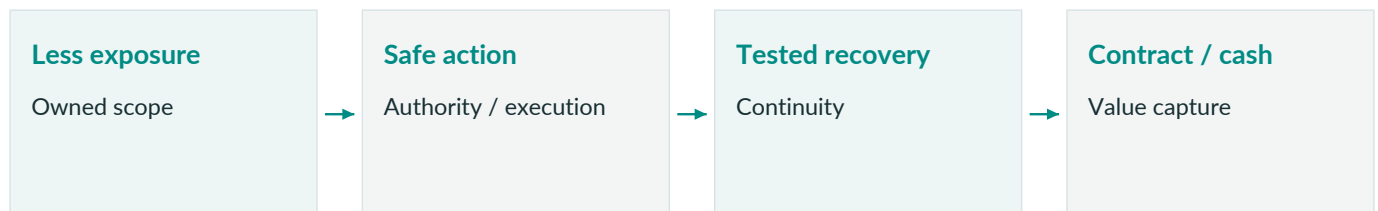
05 / SECURITY VALUE CHAIN

Security spending needs connected controls

Look at the links among exposure, authorization, response and recovery rather than a single-product replacement story.

NIST links detection, response and recovery to organizational risk management. Basel principles cover dependencies and third parties. [6] [8] TradeLens translates these concepts into opportunities and measurable outcomes.

Investment area	Operational output	Evidence of improvement
Exposed assets / vulnerabilities	Owned asset inventory and risk-based remediation	Unmanaged assets; age of unresolved high-risk items
Identity / authorization / APIs	Access limited to the required users, devices and data	Excessive privileges, authorization tests and false blocks
Detection / response integration	Evidence-backed alerts linked to authorized actions	Validation/containment time, manual waits and recurrence
Recovery / continuity	Recovery validated across data and dependent services	Recovery time, data integrity and actual business tests



Conceptual value chain. It does not show spending shares or the actual procurement sequence at Korean institutions.

“Operations matter” does not mean equipment is unnecessary

This is not an argument to eliminate security appliances. When existing tools sit in disconnected data, permission and accountability structures, integration and testing may be the priority. The better use of capital depends on the current estate and its bottlenecks.

Conditions for value capture

Platforms, integrators, managed services and recovery specialists can play different roles. A broader scope brings opportunity, but also integration expense, responsibility and support commitments. Read delivery costs alongside the contract.

06 / RESPONSE-TIME LAB

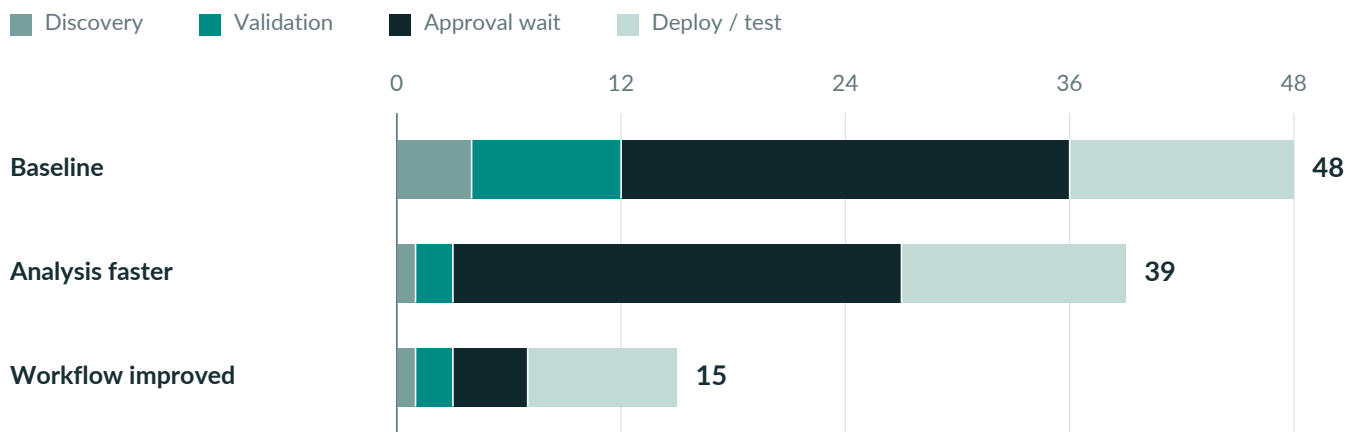
Faster analysis may only cut 48 hours to 39

Illustrative model | Compare partial automation and workflow redesign on the same elapsed-time basis.

Model A | Elapsed time to remediate one vulnerability

Baseline: discovery 4 hours + validation 8 + approval wait 24 + deployment/testing 12 = **48 hours**. Stages are sequential and non-overlapping. These are not bank observations, labor-hours or contractual targets.

Hours · illustrative assumptions



Assumed scenario	Find / validate / approve / deploy	Total	Reduction
Baseline	4 / 8 / 24 / 12 hours	48 hours	—
Analysis accelerated	1 / 2 / 24 / 12 hours	39 hours	18.8%
Workflow improved	1 / 2 / 4 / 8 hours	15 hours	68.8%

Calculations: $(48-39)/48=18.75\%$; $(48-15)/48=68.75\%$. Stacks add elapsed stage times. Parallel work, retries and recurrence are excluded.

How this changes purchasing criteria

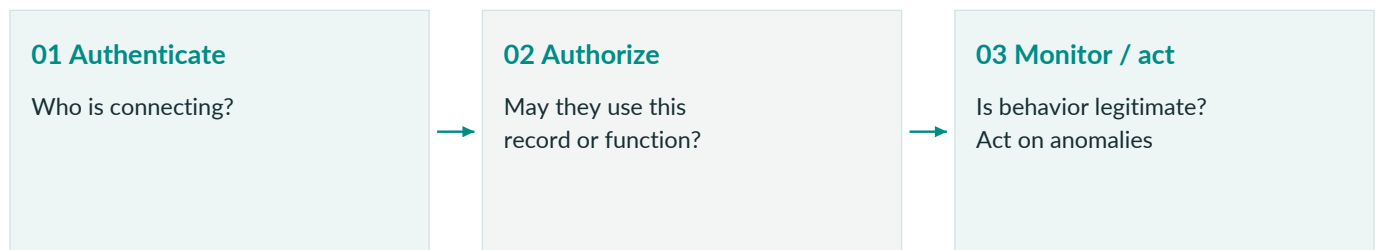
A feature that accelerates analysis has a different economic effect from a service that also improves ownership, permissions, approval and safe deployment. Shorter approval waits should come from defined authority and validated procedures—not removal of controls.

07 / IDENTITY & API CONTROL

Successful login does not grant access to every record

Network access, user authentication and authorization to specific data are separate controls.

OWASP's API guidance calls for authorization checks in functions that access individual data objects. [7] Being authenticated does not establish the right to read or change a particular record. The diagram is a general control model, not a reconstruction of the Korean incidents.



Control layer	Question to answer	What another layer cannot replace
User / device identity	Who is connecting, on which device?	An identified user still needs a defined data-access scope
Business / data permission	May this person use this record or function?	Network admission does not guarantee object-level authorization
Behavior / operations	Is permitted access being used abnormally?	After-the-fact detection does not replace authorization in design and code

Follow the data boundary, not the product boundary

Web/API protection, identity/device controls and application authorization are complementary. The bank needs a working combination across exposed and support systems, not a single label. Test permissions before and after deployment and measure legitimate activity blocked.

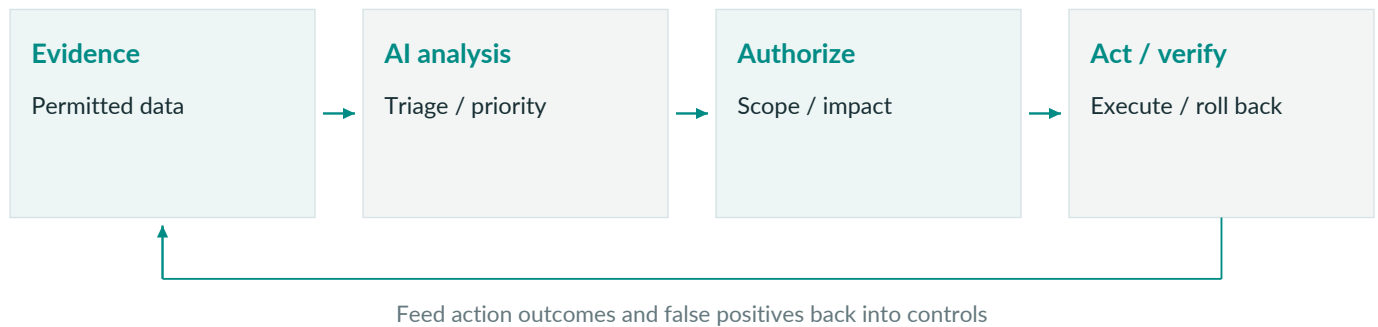
Commercial implication

Designing, integrating and testing permissions against business needs has a different cost structure from selling a product. Separating implementation from recurring operations clarifies contract obligations and the value of ongoing service.

08 / AI IN DEFENSE

Defensive AI matters when it can act safely

Automation without a defined action boundary can create new operational risk.



TradeLens operating design informed by NIST's detection, response, recovery and organizational roles. Not an agency certification or a specific product architecture. [6]

Design element	What must be settled before action
Data and evidence	Which logs and information may enter the model? Can the original evidence behind a judgment be retained?
Action authority	Separate read/analysis from blocking accounts or changing systems. Define approval for high-impact actions.
Safeguards	Validate false blocks, preserve change history, and provide rollback and manual fallback.
Evaluation	Measure misses, false positives, legitimate transaction impact and total response time—not detection alone.

An announcement is not recognized revenue

In May 2026, the FSC announced a conditional approach to easing network-separation rules for security-purpose AI use. [10] An announcement is not blanket authorization or completed procurement. Deployment still depends on applicable conditions, data handling, architecture and institution-specific procedures.

A supplier's practical differentiation

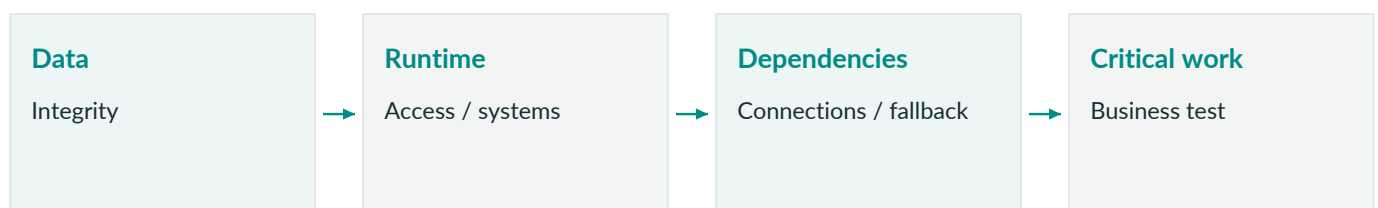
Model scores are not enough. A solution must meet customer data/deployment constraints, work under limited permissions and recover safely from mistakes. Pricing and contracts must account for the cost of making that possible.

09 / RESILIENCE & THIRD PARTIES

Buy recovery as well as the ability to block

Resilience is the ability to keep critical work available—not simply to possess backups.

In August 2026, the FSB highlighted response/recovery capacity and critical third-party resilience in discussing frontier-AI cyber risk. [9] Basel principles likewise emphasize mapping the internal and external dependencies that support critical operations. [8]



What must recover together	Outcome to validate
Data / transaction state	Not merely a backup's existence, but integrity at the required recovery point
Identity / permissions / runtime	Only the required people and services can access and operate the restored environment
External services / connections	Alternatives, failover and communication work when a critical provider fails
Customer-facing critical work	Business testing confirms that processing and controls function together

Outsourcing does not make risk disappear

Shared services can improve efficiency and visibility while concentrating dependencies. Adding providers alone does not create resilience either. Test interdependencies and switching options, and define responsibility and response contacts. This does not infer a specific bank's outsourcing design or incident cause.

Economic interpretation

Recovery exercises and integration tests can support recurring services. But unlimited response obligations or vague recovery commitments may absorb revenue in staffing, liability and standby costs. Price the service level and the responsibility together.



10 / SUPPLIER ECONOMICS

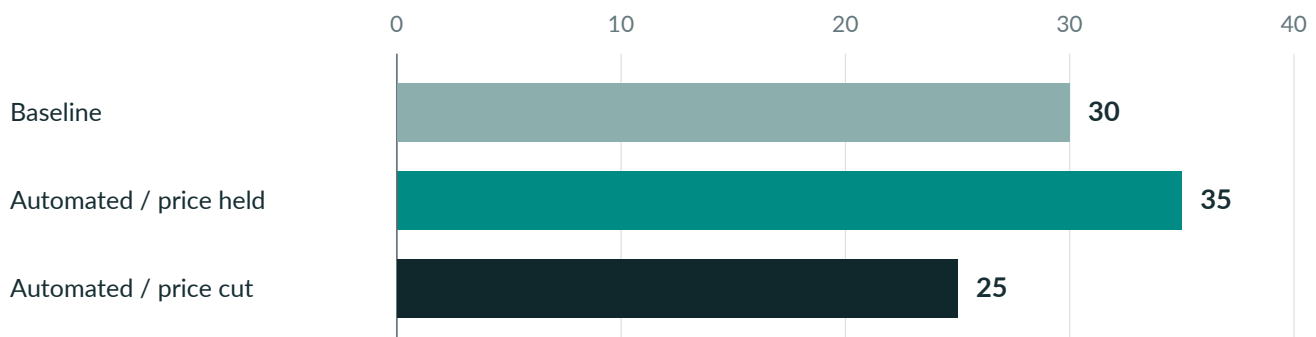
Automation does not guarantee higher profit

Illustrative model | Separate annual contract revenue from direct customer-delivery costs.

Annual assumptions • KRW m	Baseline	Automated / price held	Automated / price cut
Contract revenue	100	100	90
Direct compute / tools	10	20	20
Direct operating labor	40	25	25
Direct customer support	20	20	20
Total direct delivery cost	70	65	65
Customer contribution	30	35	25

Customer contribution

KRW m/year • illustrative



Contribution = contract revenue minus directly attributed customer-delivery costs. It is not net profit after shared R&D, administration, selling costs and tax. These are not actual vendor prices, costs or margins.

Who keeps the time saving?

Compute/tool costs rise by 10 while labor falls by 15, reducing direct cost by 5. If the fee falls by 10, contribution drops from 30 to 25. Time saved may also be redeployed to other work or customers rather than immediately reduce cash payroll.

Business evidence to follow

Paid deployment and renewal establish demand. Compute usage, operating time and support cost establish unit economics. Price retention, implementation-cost recovery and collection must connect before recurring contracts become sustainable cash flow.

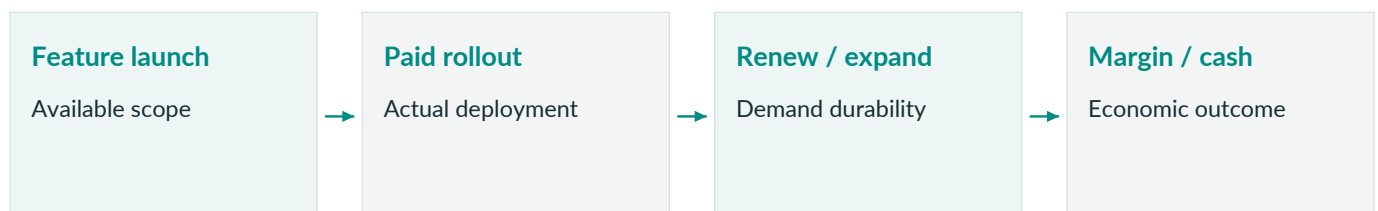
11 / KOREAN SUPPLIER MAP

Read the supply scope—not the “AI security” label

Official product descriptions illustrate business exposure, not incident-related orders or bank relationships.

Company / product	Scope described by the company	What to connect to business performance
AhnLab AhnLab XDR [11]	Detection/response integration, exposure management and AI analysis	Customer expansion, data integration, operating and support costs
IGLOO Corporation SPiDER SOAR [12]	Playbook-driven response automation and cross-product integration	Actual automated actions; implementation versus recurring-service scope
Genians Genian ZTNA [13]	Network access informed by user and device context	Covered assets, renewals and policy cost; object-level API authorization is separate
Penta Security WAPPLES [14]	Web application and API protection	Covered services, false blocks and maintenance-service terms

Industry examples irrespective of listing status—not a ranking or stock recommendation. Company feature claims do not independently establish adoption, efficacy or profitability in banking.



The same demand shift does not create the same earnings

Licenses, subscriptions, integration projects and staffed or remote managed services recognize revenue and incur costs differently. A bank incident cannot be converted directly into any of these firms' sales. New features are distinct from paying customers, renewals and cash collection.

TradeLens distinguishes business structures, not share-price winners

A high recurring-revenue share is not sufficient. Price retention, compute/labor control, manageable customization and clear responsibility must also hold. Undisclosed orders, customer relationships and margins are not filled in with assumptions.

12 / OUTLOOK & MONITORING

Follow risk reduction to locate investment value

The base view is selective expansion and reallocation—not a market growth-rate or vendor-earnings forecast.

What to monitor	Evidence strengthening the view	Evidence weakening it
Demand realization	Budget approval → paid deployment → renewal	Emergency assessments do not lead to further adoption
Security operations	Less exposure and waiting, with false-block control	Alert volume rises but effective action stalls
Recovery / dependencies	Critical work and external connections pass recovery tests	Backups exist but services cannot be restored
Supplier economics	Pricing and direct delivery/support costs sustain contribution	Price pressure overlaps with higher compute or labor expense

Base path | Selective investment in connected controls

If exposed-asset reviews lead to ongoing authorization, response and recovery operations, recurring-service opportunities broaden. If action remains one-off or merely reallocates budgets, not every supplier gains incremental revenue.

Falsification | Better technical scores are not enough

If AI improves defense and competition passes savings into lower prices, institutions may obtain better security while suppliers earn less. False positives and false blocks can also bring manual review and support costs back into the workflow. Both outcomes weaken the commercial case for automation.

Final assessment

Bank incidents establish the need for security, not the industry's profit. The AI-era investment test is the ability to connect discovery with safe action and recovery. Economic value remains where demonstrable outcomes become contracts supported by sustainable delivery costs.

Subsequent disclosures can change the interpretation of individual incidents. Illustrative models are not incident measurements or company forecasts. Institutional and company statements retain their dated scope.



13 / SOURCE REGISTER

Connect incident evidence and technical principles to their sources

Select a teal citation, a source title or “Open source” to open the original material.

01. Financial Services Commission Response to recent cyber threats in the financial sector 2026.10.02 · Official release · emergency meeting, exposed-system checks and threat sharing	Open source
02. YTN Data leaks at KB, Hana and Busan; attempts blocked at Woori and NongHyup 2026.10.02 · News report · bank statements on affected people, scale and systems	Open source
03. Economist (Korea) Customer information leaks at Shinhan, KB and Hana 2026.10.02 · News report · bank-level disclosures, including about 25,000 at Shinhan	Open source
04. NCSC and partner cyber agencies The AI shift in cyber risk: why leaders must act now 2026.06.22 · Joint statement · AI, attack/defense speed, baseline controls and readiness	Open source
05. Google Cloud · Mandiant M-Trends 2026 — Executive Edition 2026.03 · Primary incident-response research · PDF p.3; 2025 initial infection vectors	Open source
06. NIST SP 800-61r3: Incident Response Recommendations and Considerations 2025.04 · Official guidance · printed pp.5–9; detect, respond, recover and organizational roles	Open source
07. OWASP API1:2023 — Broken Object Level Authorization 2023 · Technical reference · authorization checks for access to individual objects	Open source

Separate resilience principles, institutional plans and vendor claims

08. Basel Committee · BIS Principles for Operational Resilience 2021.03 · Official principles · printed pp.6–7; dependencies, third parties and incident management	Open source
09. Financial Stability Board FSB Chair warns of risks arising from frontier AI models 2026.08.31 · Official release · Chair's assessment; response, recovery and critical third-party resilience	Open source
10. Financial Services Commission Financial-sector AI transition and planned network-separation easing 2026.05.26 · Official announcement · 22 May meeting; conditional plan for security-purpose AI use	Open source
11. AhnLab AhnLab XDR: broader visibility and AI for security operations 2026.08.26 · Company description · XDR, exposure management and AI analysis scope	Open source
12. IGLOO Corporation SPiDER SOAR As of 2026.10.03 · Official product description · playbooks, integration and orchestration	Open source
13. Genians Genian ZTNA As of 2026.10.03 · Official product description · identity/device-aware network access	Open source
14. Penta Security WAPPLES As of 2026.10.03 · Official product description · web application and API protection	Open source

Source scope: incident reporting and bank statements are distinguished from official supervisory announcements. Foreign investigation data is not pooled with domestic incidents or treated as an estimate of AI's causal effect.

Methodology, disclaimer and use of this report

Distinguish incidents, institutional/company statements, TradeLens judgments and illustrative calculations.

Item	Basis
Dates / incidents	Analysis date: 3 October 2026. Domestic incidents reflect 2 October reporting and bank statements, subject to subsequent findings.
Samples / source types	Mandiant figures cover 2025 investigations—not AI's causal impact or breach probability for all Korean institutions. Institutional/vendor statements retain their dated scope.
Model A · page 7	Sequential sum of elapsed stage times; parallel work and retries excluded. Not labor-hours or measured bank response performance.
Model B · page 11	Annual assumed fees, direct compute, labor and support. Contribution is before shared costs/tax and is not a vendor forecast.
Scope	Industry structure, operations and business economics in financial cybersecurity. No trading calls, timing, target/fair prices or personalized investment advice.

Charts and diagrams are recreated by TradeLens and do not imply source-institution approval. Calculations are rounded for display. This report is not a penetration test or a security certification.

Disclaimer

This report provides general information on technology, industries and business structures, growth and profitability. It does not provide buy or sell recommendations, trading timing, fair values, target prices or personalized investment advice. Information and analysis are as of the stated date; accuracy, completeness and currency are not guaranteed. Outlooks, estimates and illustrative calculations are uncertain. Neither investment principal nor returns are guaranteed.

Investment decisions remain the user's responsibility. Except where liability is imposed by applicable law, TradeLens is not liable for investment losses arising from use of this report.

Copyright and use restrictions

The text, charts, design, editing and structure in which TradeLens holds rights are protected by applicable law. Apart from personal reading and storage, no part may be modified, edited, translated, adapted, reproduced, transmitted, reposted, redistributed or sold without prior written permission. This applies to free and paid distribution and to all formats, including files and screenshots. Removing logos, source references or rights notices, or distributing the material under a third party's name, is prohibited.

Uses permitted by law and the separate licensing terms of third-party materials remain applicable. Please share the original link to the official TradeLens publication page.