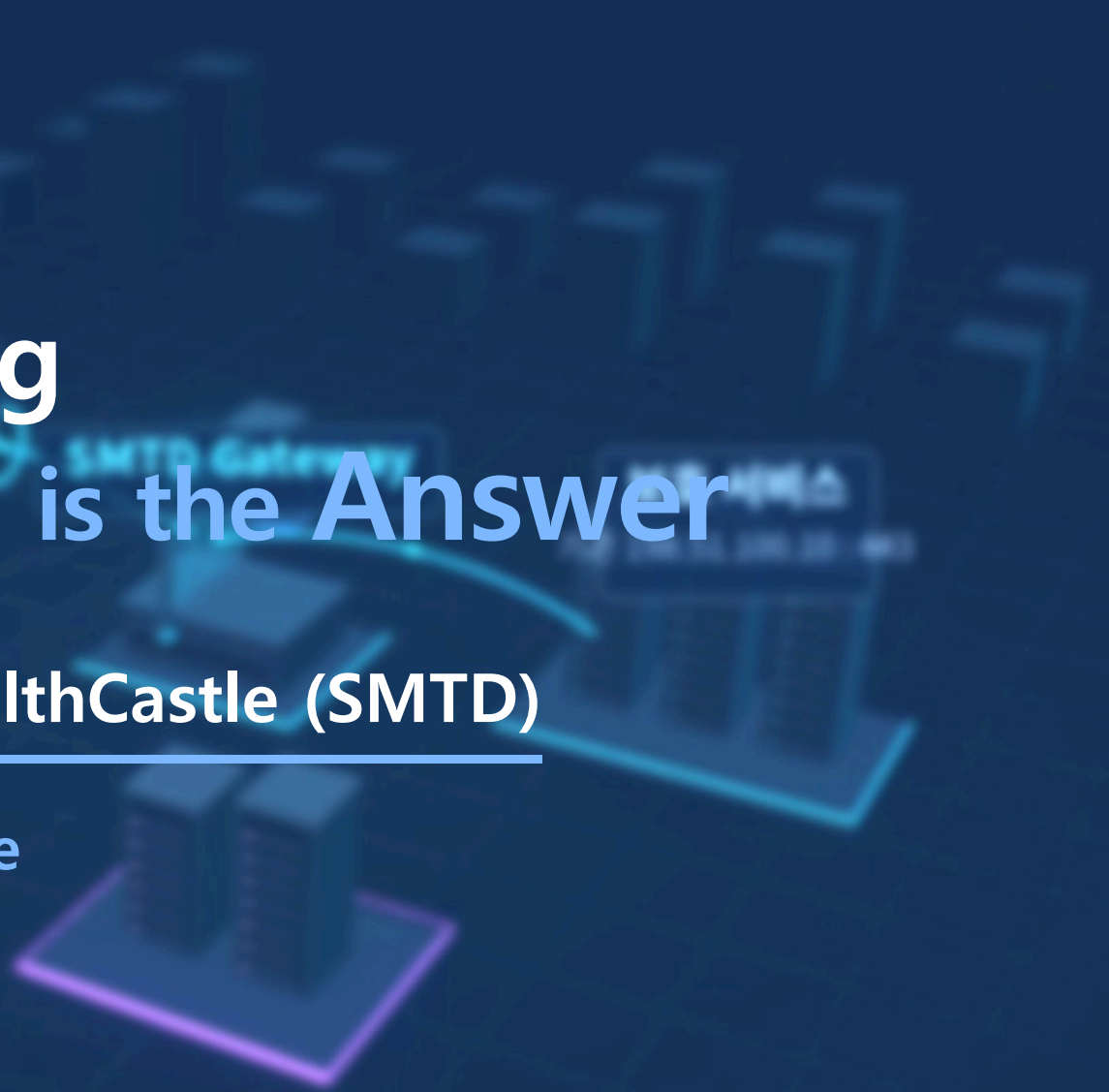
STEALTH SOLUTION Inc.

AI-Driven Hacking 'Active Defense' is the Answer

"Field-Tested Solution" StealthCastle (SMTD)

Stealth Moving Target Defense



AI-driven hacking: the attacks have already begun

Spreading across finance — companies in every industry on alert

Hacking damage in Korea and abroad, Sep–Nov 2026 (as reported)

Financial firms

37

Banks · securities · insurers, etc.
About 470,000 records leaked

Companies

110K

Customers exposed in an ERP vendor hack
Platform · construction · cosmetics, etc.

Overseas

$6.3B

Binance hack

Sources: News1 2026-11-06 (37 financial firms · 473,000 records); Seoul Economic Daily 2026-10-26 (ERP); TRM Labs 2026-10-29 (Binance)

External 'touchpoints' are 'AI's attack path.'

Company	Attack path (the external touchpoint breached)
Bank AA	Remote-access network for staff and loan agents — AI penetration agent (ARTEX) used
Securities firm BB	Partner-access network — heavy traffic disguised as normal signals
Crypto exchange CC	Mobile groupware run by an outsourcer — customer and staff data leaked
ERP vendor DD	Stolen employee VPN account — development and backup servers breached
Binance	Remote access to an engineer's laptop → hot-wallet withdrawals

Regulators now require 'a full audit of external touchpoints' and 'Zero Trust.' StealthCastle delivers both in a single product.

Note: ARTEX: open-source penetration agent chaining external LLMs such as DeepSeek
Sources: Kuki News 2026-10-14; YTN 2026-10-28; SBS Biz 2026-10-29; MTN 2026-10-26; Al Jazeera 2026-10-30; Financial News 2026-10-07

AI-driven hacking: why is it dangerous?

AI did not invent new attack methods.
It simply attacked cheaper, faster, and at far greater scale

AI share of tactics

80–90%

Humans at 4–6 decision points

Novice replication

6 min

Open model · one GPU

Fastest breakout

27 sec

Faster than human monitoring

→ **A 'dangerous world' where anyone can hack, easily, with AI, 24/7**

Sources: Anthropic threat report 2025-11-13; ZDNet Korea 2026-10-06 (Soongsil Univ. simulation); CrowdStrike 2026 Global Threat Report

Building higher walls cannot stop it

Firewall · IDS · Detection

Block after detection — too late

- Blocks only after an intrusion is confirmed
- Low-volume attempts slip under the rules

Fixed IP · Port

The map is public

- Static addresses expose attack points to recon
- Some noticed only after attack IPs were shared

Before detection, attackers must be kept from finding the door and knocking on it

Sources: Financial-sector Active Security Proposal (2026-10); New Daily 2026-10-08; Zscaler 10-K FY2026; morphisec.com; NIST SP 800-160 Vol.2 Rev.1

AI-driven hacking defense: why is 'StealthCastle' (SMTD) the "secret weapon"?

Even AI hackers cannot attack 'what they cannot find'
StealthCastle hides, trusts no one, and builds bulkheads

Sources: Financial-sector Active Security Proposal (2026-10); Company & Technology Introduction (2026-10)

'StealthCastle' Edge① New address every second

(IP·port mutation in front of assets)

Conventional — fixed target

Addresses stay the same

- An IP·port found once stays valid

StealthCastle — moving target

Addresses keep changing

- IP·ports mutate as often as **every second**

Odds of finding it: 1 in 4.2 billion

- Even if found, it changes again a second later
- Theoretical count — recalculated per customer

Note: Mutation ends at the SMTD gateway's external interface — back-end addresses and firewall policies unchanged

Sources: Company & Technology Introduction (2026-10)

'StealthCastle' Edge② Trusts no one

(Zero Trust via 5-Factor authentication)

5-Factor, verified together in the OS kernel

01	02	03	04	05
PID	**Session**	**App meta**	**User**	**Device**
Running process	Connection session	App integrity	User authentication	Device authentication

5-Factor forms an 'application identity'; unauthorized processes on infected devices are isolated

Sources: Company & Technology Introduction (2026-10)

'StealthCastle' Edge③ Bulkheads inside the castle

(App-to-App links split the inside into small segments — Micro Segmentation)

Legacy network segments

Inside a segment, all is open

- Hosts in a segment talk freely
- One breach spreads laterally

→

App to App

Only approved apps connect

- Variable multi-tunnels only between apps
- Blocks lateral movement · non-stop OT overlay

Abnormal access is lured to decoys to collect and analyze attack behavior (Optional)

Sources: Company & Technology Introduction (2026-10); Seoul Active Security Proposal §3.2 (2026-09-11)

'StealthCastle' is easy to install and use

No 'load' on systems, no added 'inconvenience' for users.

Simply 'overlay'

Layers onto existing systems as they are

- No changes to servers · firewalls · addresses
- Phased, non-stop rollout — measured per segment, then expanded

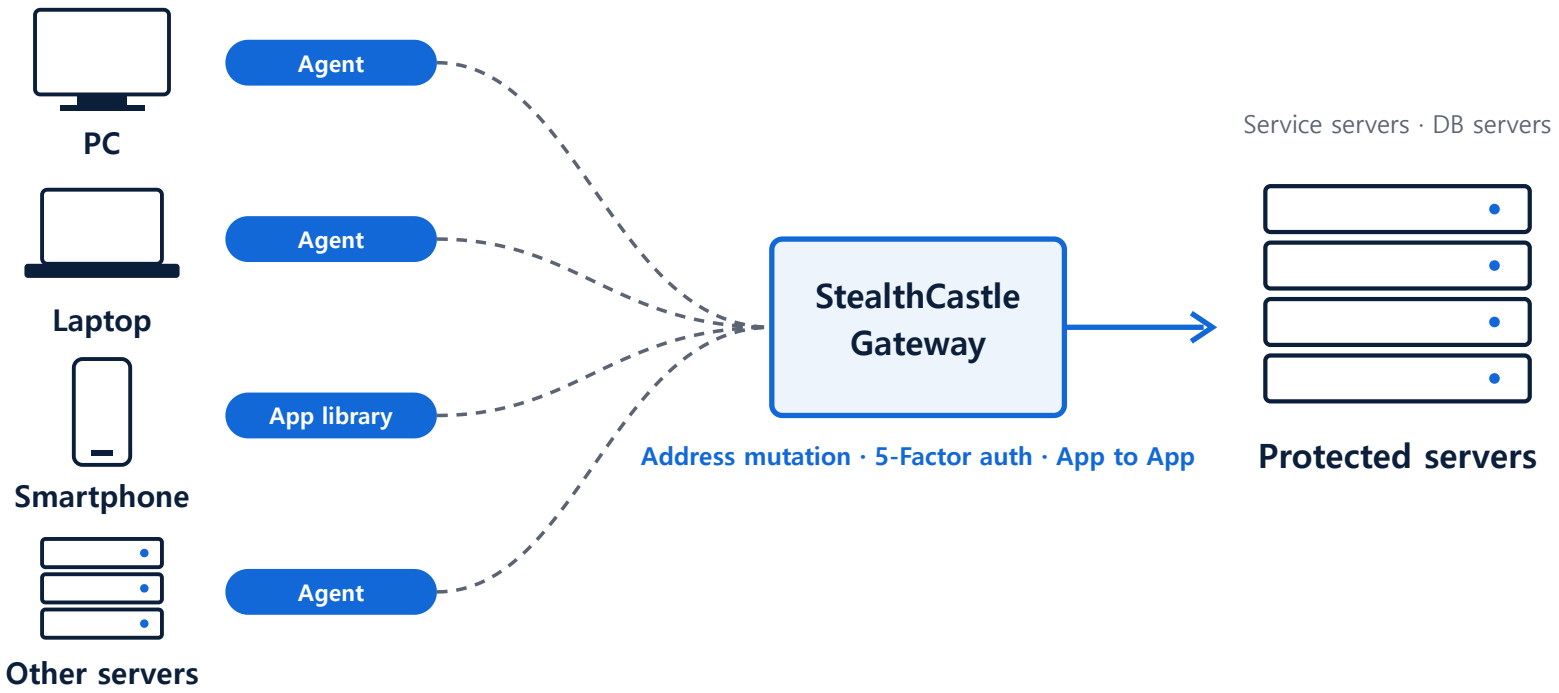
Near-zero 'overhead'

Users notice no difference after installation

- Same 40GB transfer time before/after (3,634 s) **0% latency** (throughput basis; KOIST certification test self-check)
- Seoul CCTV pilot — no lag or slowdown

Note: 0% latency is on a throughput basis — connection-setup latency (p50·p99) will be measured separately
Sources: Company & Technology Introduction (2026-10); Seoul Active Security Proposal §4.2 (2026-09-11); KOIST certification test self-check report

'StealthCastle' (SMTD) architecture



An address-mutation gateway is installed in front of the protected servers;
devices that connect (PCs, laptops, smartphones, other servers) carry an agent or an embedded app library.

(Applies to every touchpoint — staff, customer and partner networks)

'StealthCastle' — "proven by KB Kookmin Bank"

KB Kookmin Bank's red team used AI (ARTEX) for white-hat hacking

(just after the early-Oct 2026 breaches)

Test rounds

3

External network · firewall open · fixed IP

Successful attacks

0

No successful connection in logs

Round	Condition	Result
1st	Existing security + StealthCastle	Recon failed · 0 successful attacks
2nd	Existing security off, StealthCastle only	Recon failed · 0 successful attacks
3rd	**Fixed IP, ports-only mutation**	**Recon failed · 0 successful attacks**

Sources: Red-team penetration test progress report (2026-10)

"Best-in-Class Security" StealthCastle (SMTD)

Deployed by Korea's Army and Air Force, piloted by local government → expanding to finance, healthcare and enterprise in 2026

2021~22

ROKAF 20th Fighter Wing

Video surveillance active defense

2021~25

ROK Army cyber battlefield network

Auth server active defense

2023~24

Seoul CCTV pilot

0 exposed IPs·ports

2026

Finance (banks·cards)

Contracts in progress after pilots

Healthcare (a university hospital)

Forensics · security hardening consulting

Enterprise (Group A · listed Co. C, etc.)

- Zero Trust project
- Customer data protection

Korean gov't certified — NET (New Excellent Tech.) · NEP (New Excellent Product) · GS Grade 1
Procurement 'Innovative Prototype' (designation due Dec 2026; innovation · public-value review passed)
U.S. patent granted (Sep 2026) · Multiple SCI journal papers published

Note: Financial customers and Group A are not named
Sources: Company & Technology Introduction (2026-10); Seoul Active Security Proposal §4.2 (2026-09-11); IR deck; USPTO documents (2026-09)

U.S. cybersecurity vision: "Active Defense"

StealthCastle (SMTD) is an 'active defense' solution.

2011

White House NSTC

Core R&D theme

2020

NIST 800-53

Security control SC-30(3)

2026

NIST 800-172r3

MTD requirement retained

*** Since the 2010s, the U.S. has set 'active defense' as its cybersecurity vision.**
*** Memory-mutation vendors (e.g., Morphisec) exist, but a company that has commercialized network mutation is hard to find.**

Note: NIST lists it as an optional control
Sources: NSTC 2011; NIST SP 800-53r5·800-172r3; morphisec.com

Another edge: AEGIS Homomorphic Encryption (FHE)

Quantum-resistant encryption
Compute, statistics and search run without decrypting.

01
Plaintext
Original data

→

02
Encrypt
AGCD-based, quantum-resistant

→

03
Compute on ciphertext
Compute · stats · search

→

04
Decrypt results only
Originals never exposed

Privacy-Preserving Data Streaming
No one ever sees the original data during compute, statistics or search.

Sources: Company & Technology Introduction (2026-10)

AEGIS has broken through FHE's 'speed' and 'error' barriers.

Conventional lattice-based FHE

Computation takes long

- Degree-10 compute: 0.7997 s

→

AEGIS FHE

Computes fast

- Degree-10 compute: **0.0075 s**
  : over 100× faster than lattice-based
- Self-measured · not yet third-party verified

AEGIS is not lattice-based; it is homomorphic encryption built on AGCD (Approximate Greatest Common Divisor).

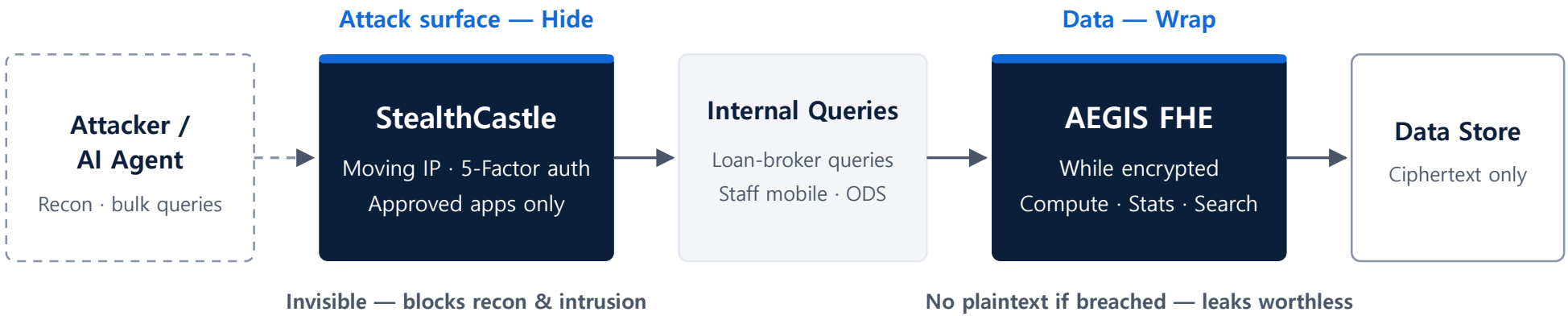
- Unlike lattice-based schemes, there is no noise — in other words, no error.
- Unlike lattice-based schemes, no noise-removing bootstrapping is needed.
- So computation is fundamentally faster.

AEGIS enables new progress in finance, healthcare and defense through Privacy-Preserving Data Processing.

Note: Measurement hardware, parameters and security level not stated in the source material
Sources: Company & Technology Introduction (2026-10)

AI hacking defense: the "best combination"

「Wrap with AEGIS, hide with StealthCastle」



StealthCastle hides the attack surface (external touchpoints); AEGIS wraps the data for use. Insiders who steal it get nothing — they take what looks like gold and find only sand.

Note: Conceptual layout — deployment zones are set during pilots
Sources: Company & Technology Introduction (2026-10)

'Proven Careers · Growing Vision' Research & Management



Yoo Han Park

CEO

- Strategy Head, Cha Biotech Group
- CEO, KBS Business
- KBS Anchor · Economics Editor
- KBS Washington Correspondent
- Fellow, Duke Univ.
- M.A. Economics, Sogang Univ.
- B.B.A., SNU



Hee Han

CSO

- Professor, Korea Univ. Graduate School of Information Security
- Director, KIDA; Principal Researcher, ADD
- Member, National S&T Policy Committee
- Science Advisor to six Defense Ministers
- Brigadier General, KDIC
- Director, Motorola Lab (T2TRC)
- Ph.D. in Electrical Engineering
- Korea Military Academy; Yonsei Univ.; Caltech; Yale Univ.



Seok-Jin Kang

Head of R&D

- Professor, SNU Math Sciences
- Fellow, Korean Academy of S&T
- Professor, Univ. of Notre Dame
- Researcher, UC Berkeley
- Ph.D., Yale Univ.
- B.S. Mathematics, SNU



Byungdo Lee

CTO

- Professor, Cheongju Univ.
- Professor, Chungbuk Provincial Univ.
- Tech Director, CyberResearch
- Center Director, ROK Cyber Command



Junhwan Kim

Auditor

- Visiting Professor, Sejong Univ.
- Asst. Governor, Korea FSS
- Head of Bank Supervision, FSS
- MBA, New York Univ.
- B.B.A., SNU



Red Team

Attack validation

- Ex-team leads, ROK Cyber Command

Note: Titles and careers confirmed by the CEO (2026-10-11), most recent first
Sources: Company & Technology Introduction (2026-10); IR deck

Sources

Area	Material
Incidents · threats	Financial News 2026-10-04·10-07 · Herald Economy 10-03 · Money Today 10-02 · New Daily 10-08 · ZDNet Korea 10-06 · CrowdStrike 2026 GTR · Anthropic 2025-11-13
Global · U.S.	Zscaler 10-K FY2026 · morphisec.com · NIST SP 800-53r5·800-160 Vol.2·800-172r3 · NSTC 2011
Company materials	Company & Technology Introduction (2026-10) · Financial-sector Active Security Proposal (2026-10) · Seoul Active Security Proposal (2026-09-11) · IR deck
Tests · patents	Red-team penetration test progress report (2026-10) · USPTO documents (2026-09)

Sources: Page-level sources grouped by area