

AI-based  
Anti-hacking & Anti-phishing solutions



May 2023

**1** We provide  
**anti-hacking & anti-phishing** solutions  
based on **AI**(artificial intelligence)

# 1. Who is Everspin?

We are leading cybersecurity industry by providing **AI-based** solutions to prevent **hacking & phishing** incidents

Every day, ever-changing security codes.

New Module

## Anti-Hacking 'Eversafe'

EverSafe's AI, which has 'infinite code' to prevent cyber-attacks, changes its security modules on its own every day to prevent hacking.

## AI Cloud Server

## Anti-phishing 'FakeFinder'

There are tens of millions of apps in the world. FakeFinder Whitelist DB prevents phishing crimes through malicious apps with information on all apps in the world collected by AI.

DETECTING

# 1. Who is Everspin?

## Market Dominance

The 3 solutions which are Eversafe-mobile, Eversafe-web, FakeFinder are dominating anti-hacking and phishing solution market

Solution	Banks	Securities	Credit Cards	Saving Banks	Insurance/Capital, etc.
<b>Eversafe Mobile</b>					
<b>Eversafe Web</b>					
<b>Fake Finder Mobile</b>					

**2** Unprecedented solutions  
were invented by Everspin

## 2. Where does hacker attack?



Could you introduce yourself?

I am a hacker.

Do you attack **server and database**?

**Ultimately, Yes**  
But...

Umm, then where do you **attack first**?

Well, we attack **website and mobile app** first.

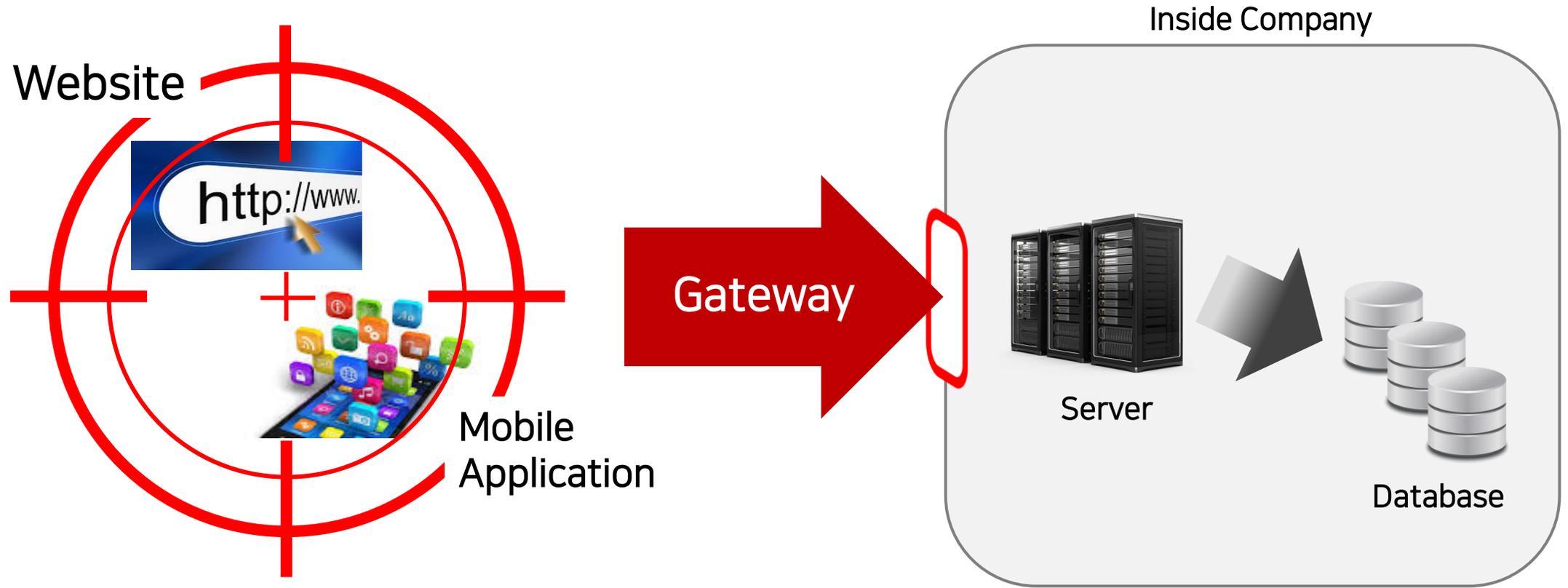
Really, we didn't know that. Why?

They are **easily accessed** by users including **hackers**.



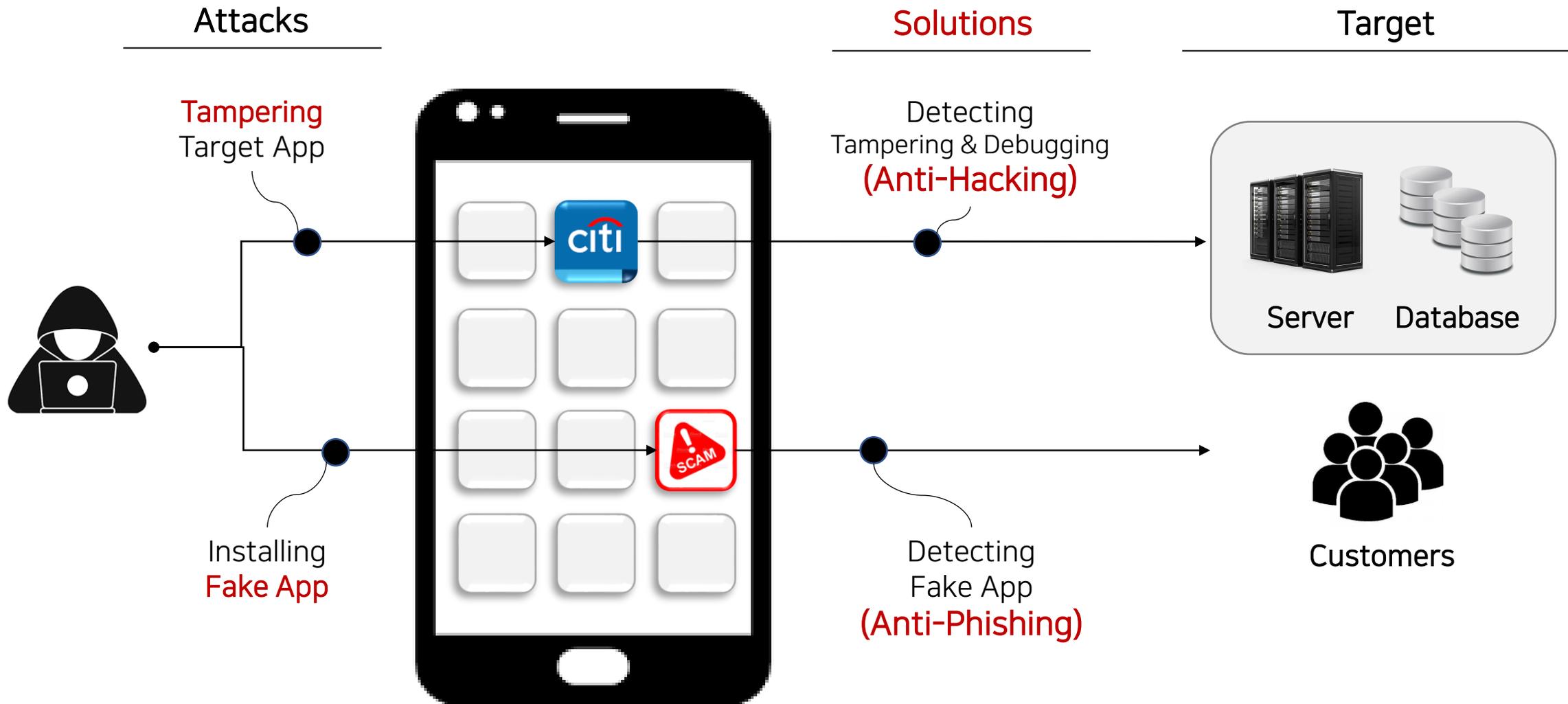
### 3. What should be protected to prevent cybersecurity incidents?

Websites and mobile apps called 'service channels' should be protected at first as a gateway of cyber-attack.



# 4. How can service channels be protected?

Anti-hacking & anti-phishing solutions are necessary to prevent all mobile app-related incidents



# 5. How does Everspin protect websites and mobile apps?

Everspin invented unprecedented solutions by **“stopping stereotyping and thinking out of the box”**

Other Vendors



Anti-Hacking Solution

“Static”

Only one security module is installed in app to detect and block hacker’s attack



“AI-based MTD(\*)”

Several security modules changing randomly are installed in app



(\*) Moving Target Defense

Anti-Phishing Solution

“Blacklist”

Very limited malicious apps are detected by malware database reported only after incidents occurred,



“Whitelist”

ALL malicious apps even before incidents occur are detected by comparing with all true apps DB collected from all official app stores



FakeFinder

(1) Anti-Hacking Solution



World's First **M**oving **T**arget **D**efense(MTD)-Based Technology

✓ Principle of Hacking

There is no unsolved maze in this World. But we only need **sufficient time** to analyze the maze.

If the hacker who understands the programming language of developers, has sufficient time, everything will be finally analyzed and bypassed.

[Problem] Is the hacker able to analyze the following code?

```
.line 57
iget-object v0, p0, Lcom/isaku/app/RegisterPinActivity;->account:Lcom/isaku/app/model/UserAccount;

iget-object v1, p0, Lcom/isaku/app/RegisterPinActivity;->newpin:Landroid/widget/EditText;

invoke-virtual {v1}, Landroid/widget/EditText;->getText()Landroid/text/Editable;

move-result-object v1

invoke-virtual {v1}, Ljava/lang/Object;->toString()Ljava/lang/String;

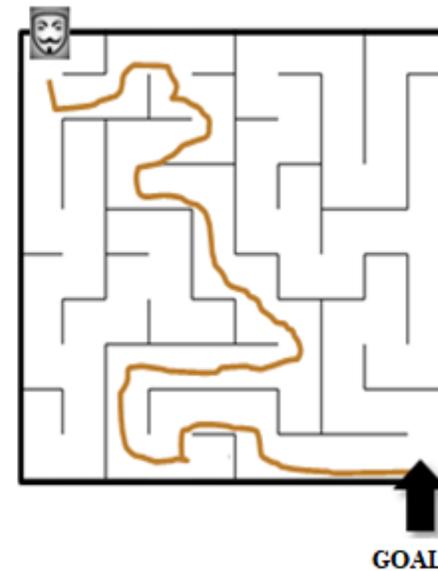
move-result-object v1

invoke-virtual {v0, v1}, Lcom/isaku/app/model/UserAccount;->setPin(Ljava/lang/String;)V

.line 59
new-instance v0, Lcom/isaku/app/RegisterPinActivity$RequestActivationCodeTask;

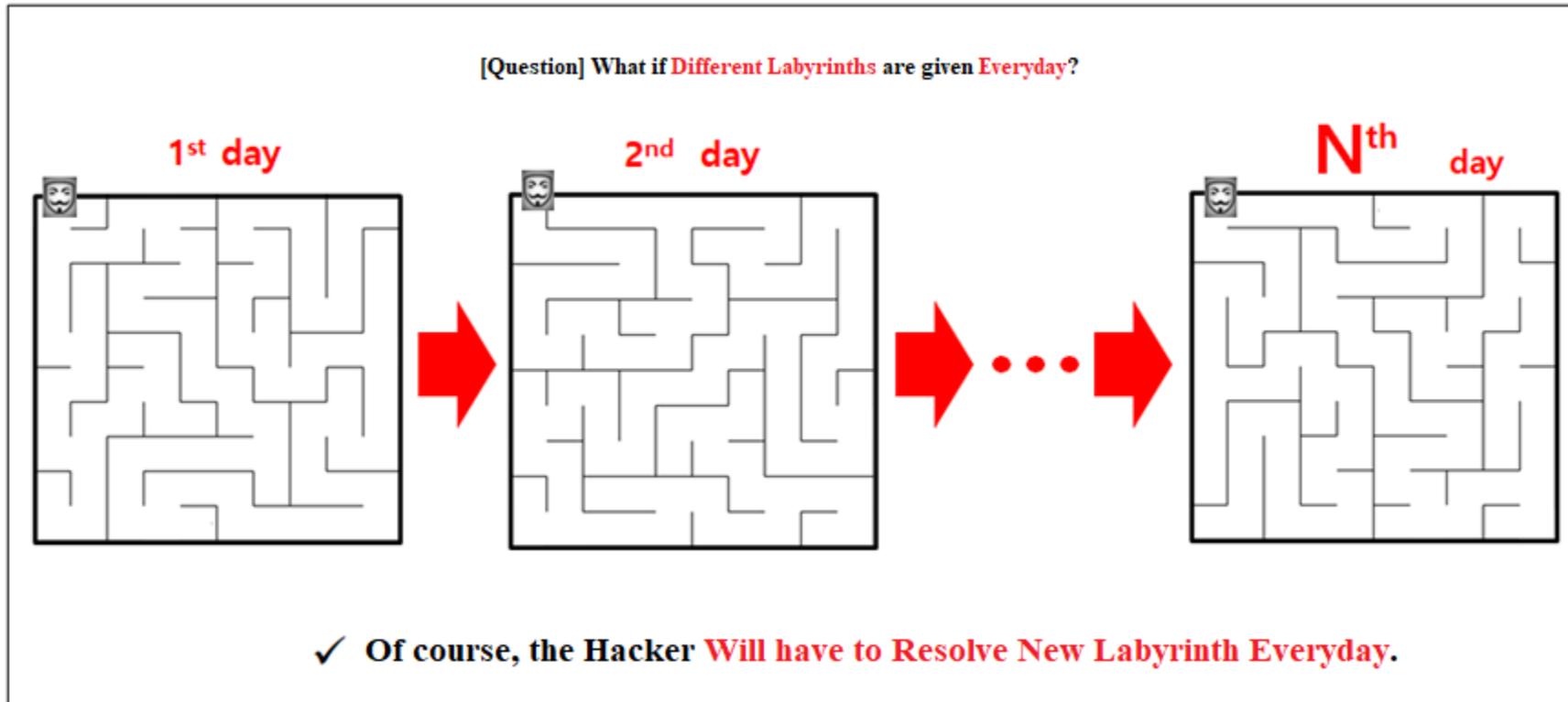
iget-object v1, p0, Lcom/isaku/app/RegisterPinActivity;->account:Lcom/isaku/app/model/UserAccount;
```

[Answer] The code is analyzed as following labyrinth with only sufficient time



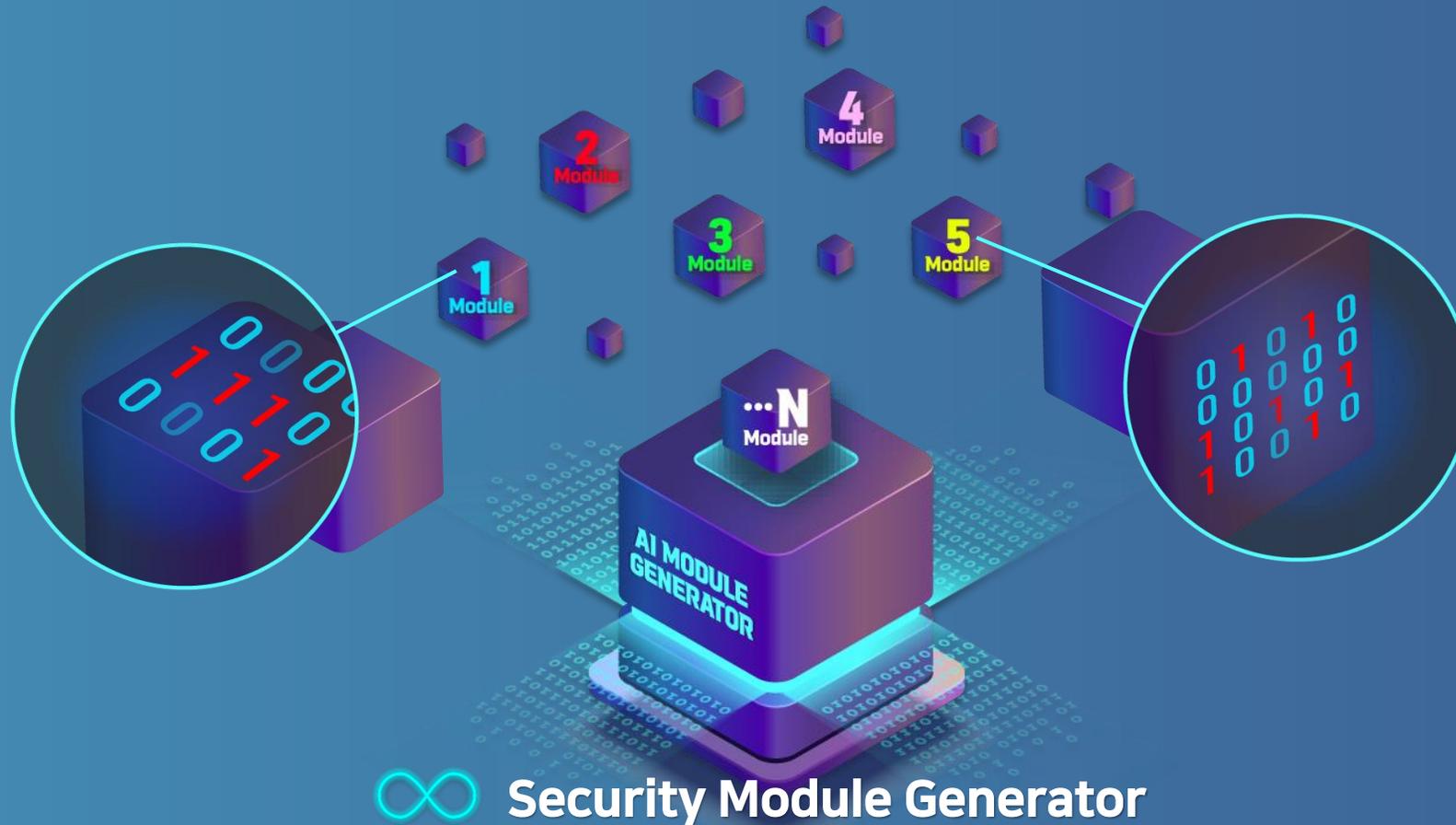
✓ Principle of Hacking

But if New Mazes are given Everyday to the Hacker as the following image, the Time of the Hacker could be controlled as the Hacker needs to resolve Different Mazes Everyday.



(1) Eversafe (anti-hacking solution) : **AI based MTD Security Module Generator**

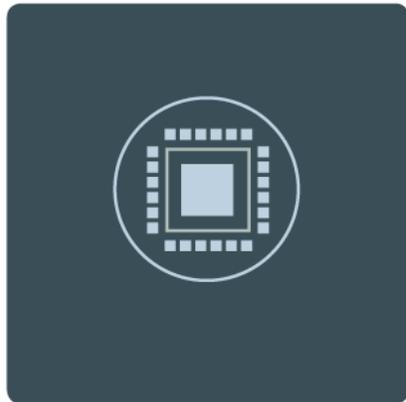
- Security module can be generated infinitely.
- Every security module has different source code.



## Conventional Security Solution

One Static (STATIC) security module keeps working with same pattern

When the single repeated pattern is analyzed, there can be found various ways to bypass the respective security module.

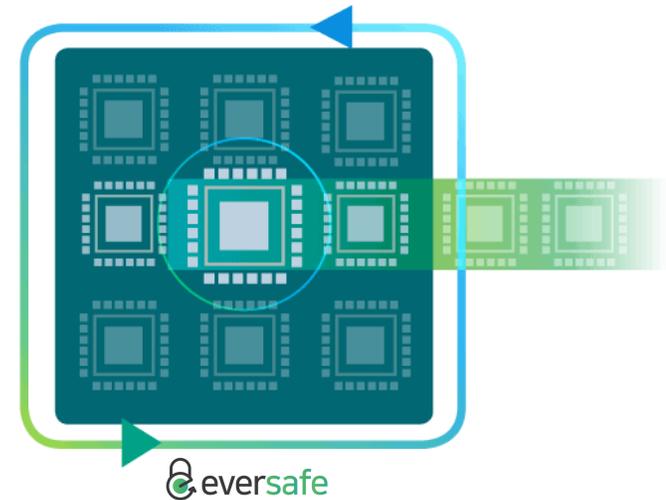


VS.

## EverSafe

Everyday the New (Moving Target Defense-based) Security Modules work with different patterns

New Security Modules are Replaced Everyday for Strict Protection, even before finishing the analysis of one single security module.



Commonsensibly, which one could be SAFER?  
Everspin is the World's First Company which Attempted and Achieved  
Commercialization of Daily Substitution of Anti-Hacking Logic.

# BMT (Benchmark Test)

- We Never Lost in Any and All Technological Competition during all BMTs.
- Moreover, We Never Lost Any and All Technological Competitive BMT against Any Other Overseas Vendors.

Only One  
Dynamic Security  
(Moving Target Defense)  
Technology in the World



Class	Clients	Competitors	Results of Technological Competitive BMT	Remarks
Overseas	 The 3 <sup>rd</sup> Largest Bank in Indonesia (No.1 Online Bank) (Listed)	<ul style="list-style-type: none"> <li>• Promon(EU)</li> </ul>	EVERSPIN <b>selected</b>	
	 The 4 <sup>th</sup> Largest Bank in Indonesia (Listed)	<ul style="list-style-type: none"> <li>• Promon,</li> <li>• Arxan(U.S.A.)</li> </ul>	EVERSPIN <b>selected</b>	Additional security assessment by third entity was performed after selection of BMT
Domestic (Korea)	 The 1 <sup>st</sup> Largest Bank in Korea (with most users)	<ul style="list-style-type: none"> <li>• Stealien</li> <li>• Secucen</li> </ul>	EVERSPIN <b>selected</b>	
	 The 3 <sup>rd</sup> Largest Bank in Korea (Listed)	<ul style="list-style-type: none"> <li>• Arxan</li> <li>• Stealien</li> <li>• BTworks</li> <li>• NSHC</li> <li>• Secucen</li> <li>• Lockin Company</li> <li>• Ahob</li> </ul>	EVERSPIN <b>selected</b>	Mutual hacking among participating competitors has been performed (for approx. 12 days)

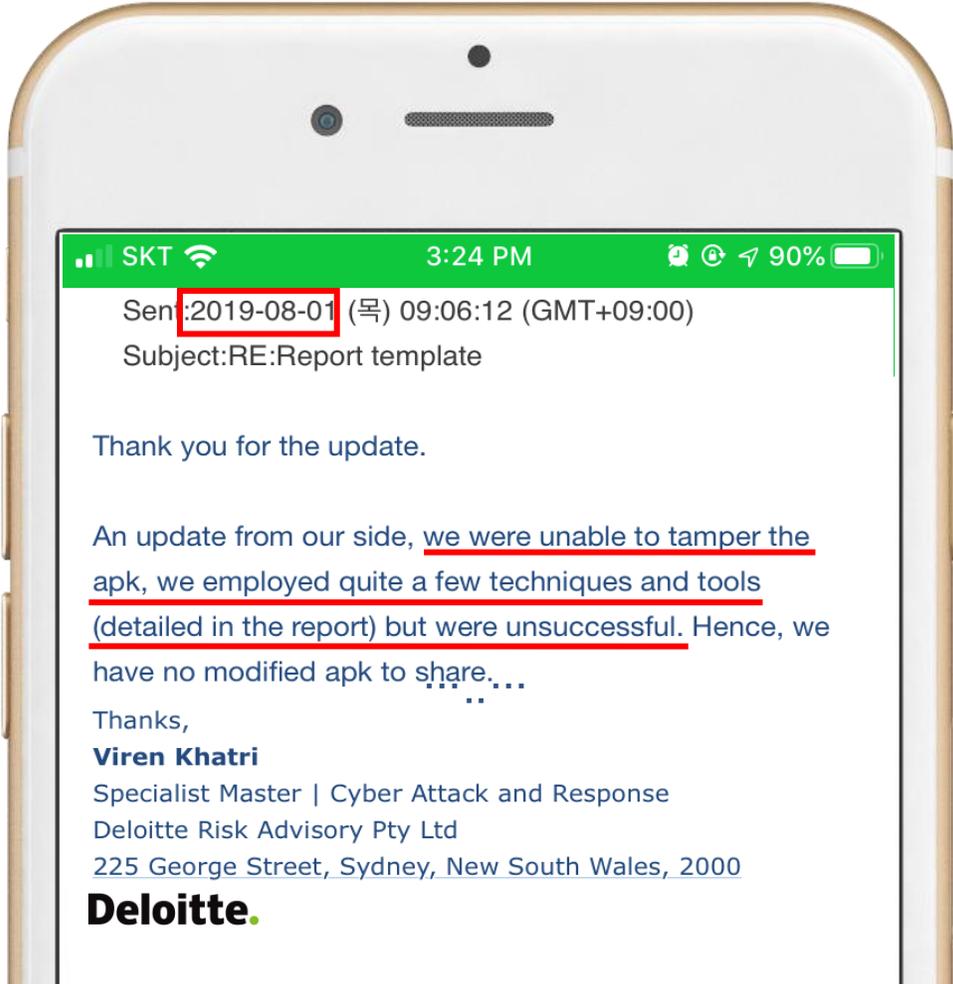
- Requesting Authority:
- Verifying Authority:



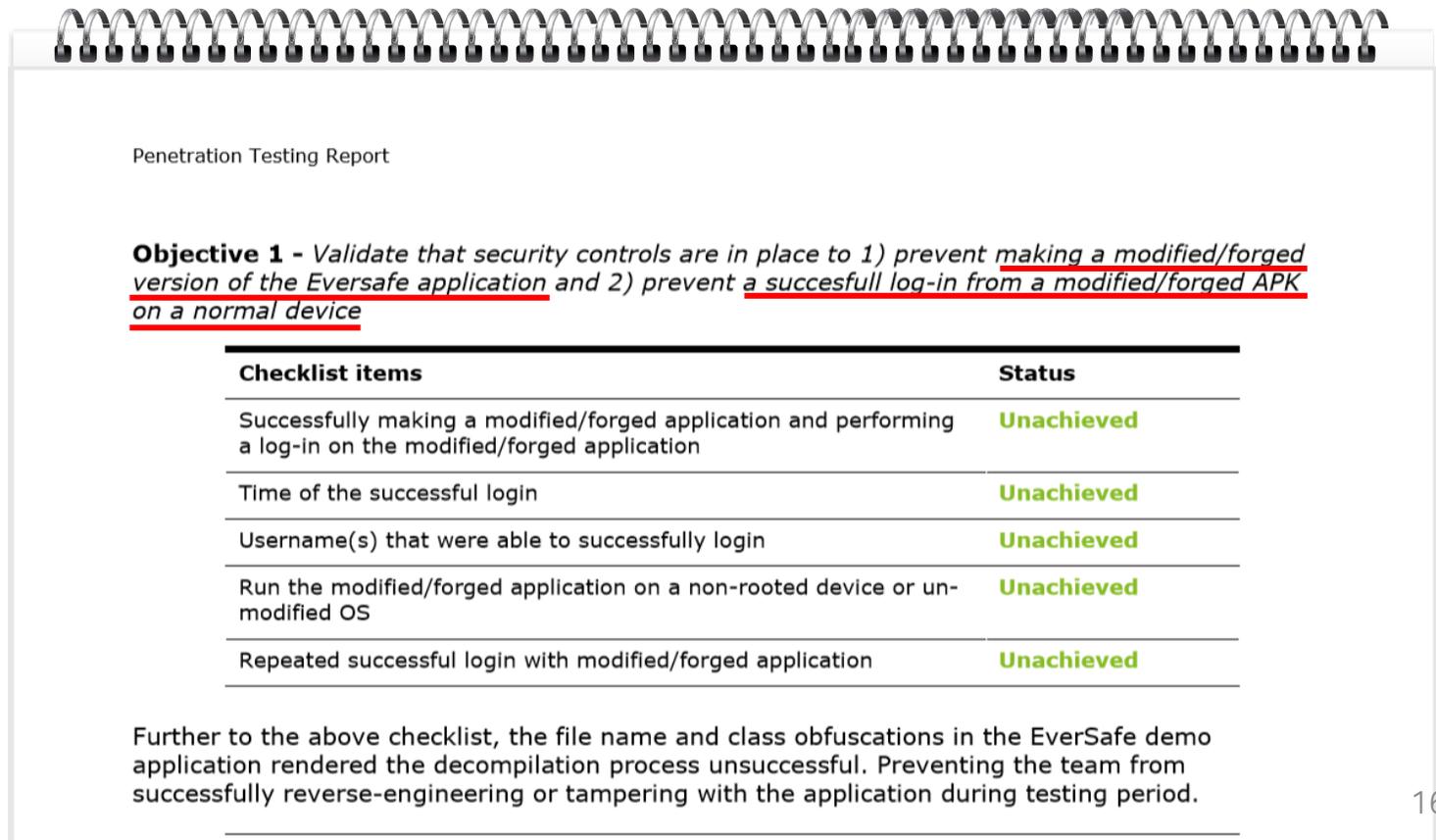
• Purpose of Request for Penetration Test:

Received Third-Party Security Assessment through Authoritative Entities with Best Expertise to decide on sequential adoption to total 150 group affiliates (50 in Japan) such as securities companies, insurance companies, banks, crypto-currency exchanges, etc. under the governance of SBI Holdings

• Results: **Flawless Full PASS** as follows



September 2019  
EverSafe Penetration Testing



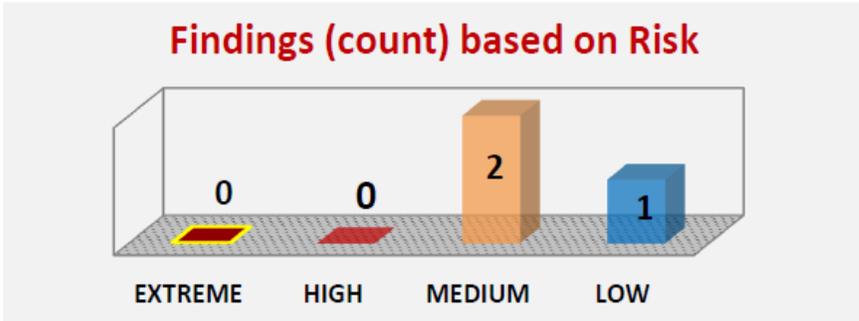
- Requesting Authority:
- Verifying Authority:



2nd Half of 2020  
EverSafe Penetration Testing

Findings Profile

The charts below show a visual overview of the results:



All the 3 security findings are listed below:

FINDING TITLE	RISK <sup>1</sup>	STATUS <sup>2</sup>
Application Findings		
Finding 1: Android: Weak Root Detection	MEDIUM	Not re-tested
Finding 2: Android: No binary protection on kr.coeverspin.eversafe	MEDIUM	Not re-tested
Finding 3: Weak Certificate Pinning	LOW	Not re-tested

- **Purpose of Request for Penetration Testing:** Mandiri Bank, the 4<sup>th</sup> largest bank of Indonesia performed the BMT on 3 companies (Arxan of U.S.A., Promon of EU and Everspin of Korea) for the adoption of Anti-Hacking solution, **and Everspin has been finally selected thanks to its technological predominance. And the third-party assessment has been requested to ITSEC, an international professional entity for the objective examination on the Everspin product.**
- **Results:** The product of Everspin PASSED the examination without any flaw in any of the EXTREME and HIGH items which are directly related to the hacking potential, while the Arxan solution which the institution was previously using, has been bypassed in few days.

General Summary of the Report

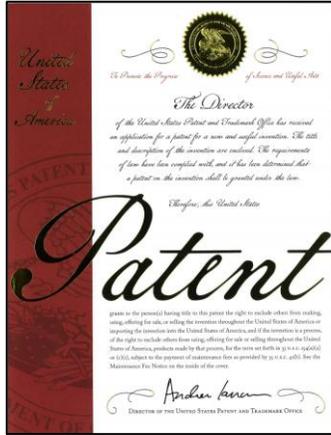
- Thanks to the APP-Server communication encryption reinforcement, the existing API communication interval could be completely bypassed within a (1) week, but the EVERSAFE only allowed bypass of few meaningless parts during 3-weeks period.
- As reverse engineering and construction of customized tool is essential when attempting to bypass EVERSAFE, the respective operations cannot be completed within the assessment period of 15 days.
- The existing solution did not have any function of malicious activity report and alarm to administrator, but EVERSAFE offers the admin function to the administrator.
- Especially, EVERSAFE technology is also applied on Web application firewall area, and additionally protects the application request between the API and the server which does not allow any network traffic analysis.

# Patent

- The Dynamic (Moving Target Defense) Security Technology of EVERSPIN is an original and unique technology which **has been registered in 11 countries around the world (33 patents)** unlike the conventional technologies limited to the boundary of Korea.



Patent of Korea



U.S. Patent



Patent of Japan



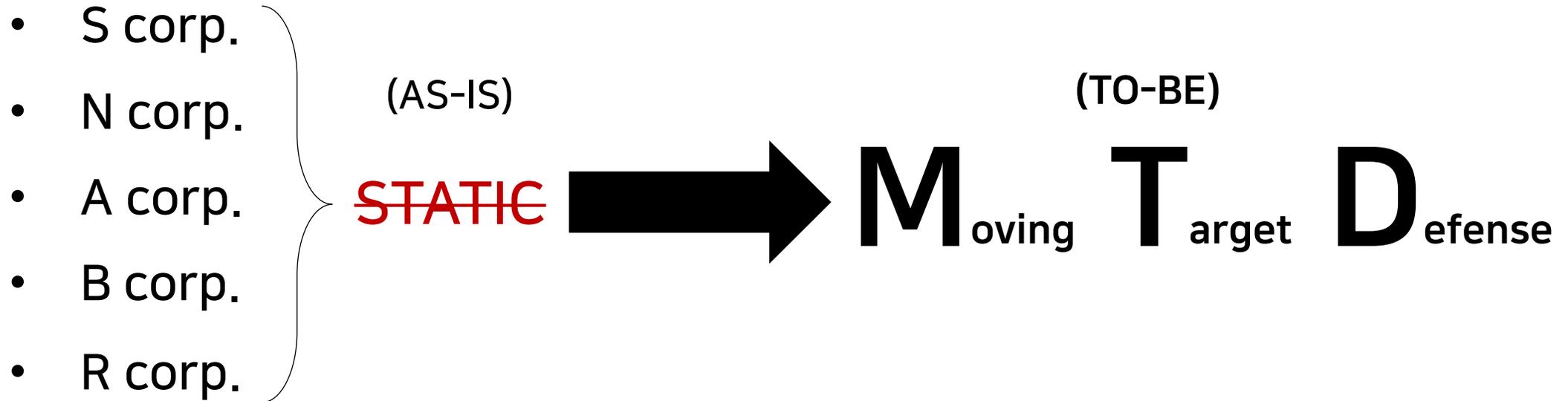
EU Patent

The technology of EVERSPIN has been registered as a patent by proving its Excellence to the Patent Offices of many countries around the world

PATENTS	Korea	U.S.A.	Japan	U.K.	France	Germany	Luxembur g	Holland	Italia	Swiss	China	India
Dynamic security module device and its operation method	Registration complete	Applied										
Creation method and device of dynamic security module	Registration complete	Applied										
Server device of dynamic security module and its operation method	Registration complete	Applied										

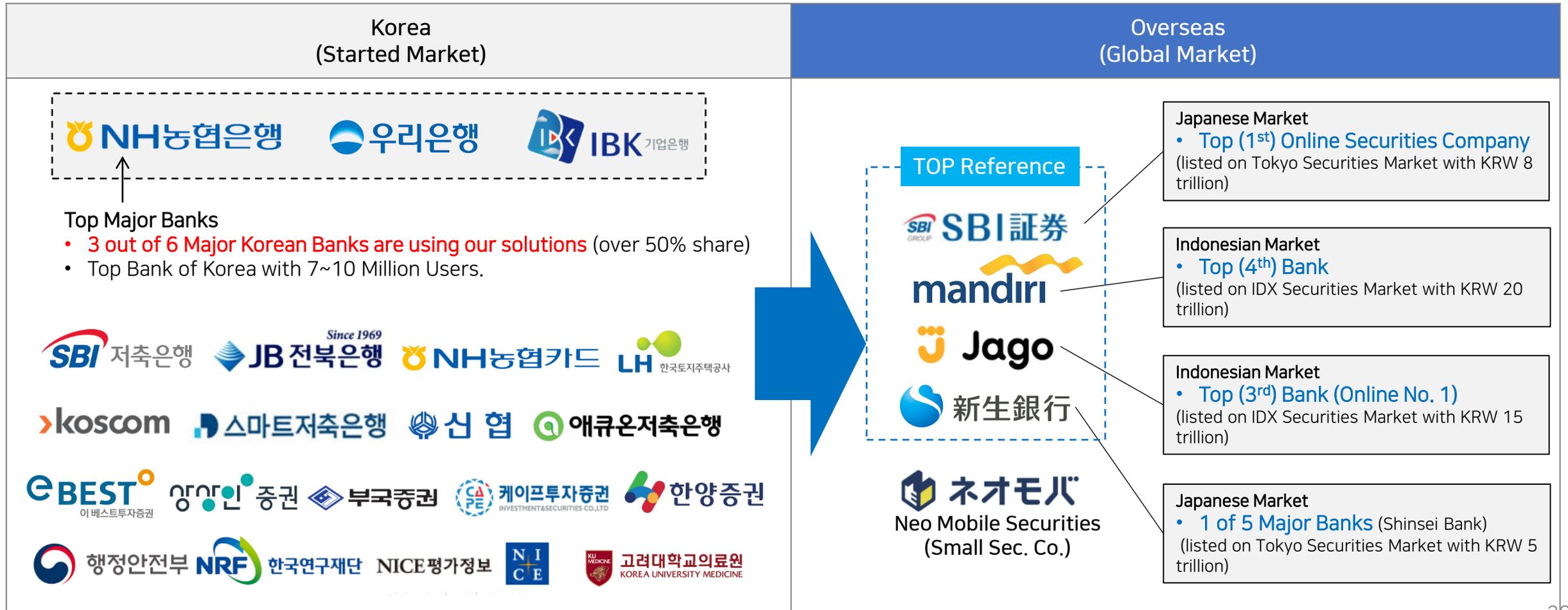
# Win-Back

All references of EVERSPIN, consist in cases of Win-Back which replaced the conventional **STATIC** technology with the new **MTD(Moving Target Defense)** Security Technology of Everspin.



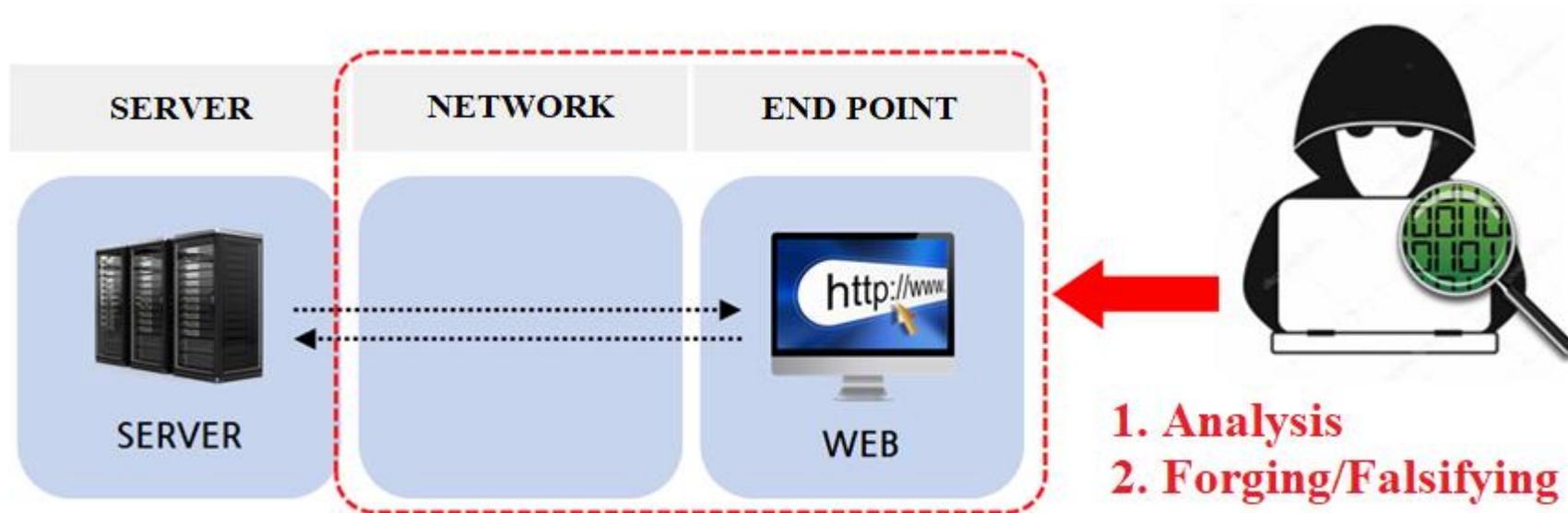
# The Only Global Security Technology in Korea

- Over 50% of major banks of Korea, Upgraded and Replaced their conventional STATIC technology into the MTD (Moving Target Defense) Technology of EVERSPIN.
- EverSafe, is the **Only Global Security Technology of Korea which is applied in overseas major financial institutions** beyond the boundaries of Korea.



# **Extended** Area (Web)

- Everspin extended to **WEB Area (PC & Mobile)** in addition to mobile area, through endless R&D on the Moving Target Defense Technology (released in January 2021)
- Woori Credit Card hosted a competitive technological BMT between EverSafe and Arxan of U.S.A., EverSafe WON OVERWHELMINGLY.
- Korea Investment & Securities Co., Ltd. hosted a competitive technological BMT between Eversafe and Imperva(\*) of U.S.A., again, Eversafe WON OVERWHELMINGLY.  
 (\*)Highest Class in the World of Web Security: <https://en.wikipedia.org/wiki/Imperva>



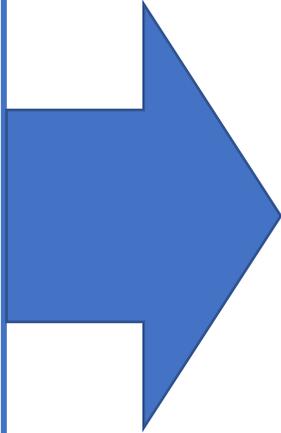
We have Extended the Dynamic (Moving Target Defense) Security Technology even to the WEB area to Completely Block the Analyzing and Forging Act of the Hacker in the WEB, where hacking attack is very frequent.

- Moving Target Defense-based Anti-Hacking Technology performs protection by changing the security code that detects hacker’s analysis and forgery by daily or weekly basis.
- 'EverSafe WEB' is an Anti-Hacking Solution which does not give enough time to the attempt of hacker of analyzing and hacking the Web.

```
574+1797))=LlUxh());else if(!!![[]]){_pHAib[_nLKZG(__D
488+1864)}]=_nLKZG(__DWchT[669%894+1123])+_nLKZG(__DW
())[_nLKZG(__DWchT[604%174+800])+_nLKZG(__DWchT[721*90
){if(!!!!!!![[]]){_pHAib[_nLKZG(__DWchT[490+577-619])}
((920*486)+32658,137*2+38113);}else{_pHAib[_nLKZG(__D
561956)}]=9223(398-97+41300>>717%847+43460);}else if(!!
521+809)}]=_nLKZG(__DWchT[934+286-901]}]=_nLKZG(__DWch
129831)}+_nLKZG(__DWchT[635+333-563]}]=_nLKZG(__DWch
{_pHAib[_nLKZG(__DWchT[(453^2)+869])+_nLKZG(__DWchT[
[]){_pHAib[_nLKZG(__DWchT[165%244+1719])+_nLKZG(__DW
287311)}]=YYBPN78747();}else{_pHAib[_nLKZG(__DWchT[(8
66+87495);if(window[_nLKZG(__DWchT[70%871+453])+_nLK
if(!!!!!!![[]){_pHAib[_nLKZG(__DWchT[398%895-10])+_nL
{_pHAib[_nLKZG(__DWchT[27*969-25161])+_nLKZG(__DWch
{_pHAib[_nLKZG(__DWchT[(515^409)+80])+_nLKZG(__DWchT
60)}+_nLKZG(__DWchT[882%368+47]);}else{if(window[_nL
[_nLKZG(__DWchT[645/65+810.0769230769231]}+_nLKZG(__D
[]){_pHAib[_nLKZG(__DWchT[675*694-467499])+_nLKZG(__
JSON());}else{_pHAib[_nLKZG(__DWchT[61+540+350])+_nL
626407>867*276-184713);}else if(!!!!!!![[]){_pHAib[_nL
142749]}+_nLKZG(__DWchT[936/693+405.64935064935065]}]=
(_nLKZG(__DWchT[107/742+604.855795148248]))(781+30+58
60968)}+_nLKZG(__DWchT[624/690+466.09565217391304]})(8
(nu11.eEwsX);}else{_pHAib[_nLKZG(__DWchT[662*426-2814
(401/663+44191.395173453995,56+40+38291);}else if(!!![
JSON());}if(new window[_nLKZG(__DWchT[166-993+2713]}
293)}+_nLKZG(__DWchT[542/185+316.07027027027027]})=hH
174277)};else{_pHAib[_nLKZG(__DWchT[650*970-630041]}
if(!!!!!!![[]){_pHAib[_nLKZG(__DWchT[(397^964)-510]}
582757)}+_nLKZG(__DWchT[272-840+15871]}]=JSON.parse('f
```

Actual security script provided to Client A (part of source code)

Dynamic Change Factors(*)	
<input checked="" type="checkbox"/>	Automatized tool detection code
<input checked="" type="checkbox"/>	Integrity detection code
<input checked="" type="checkbox"/>	Identifier
<input checked="" type="checkbox"/>	Function location
<input checked="" type="checkbox"/>	Factor sequence, return value use method
<input checked="" type="checkbox"/>	Encryption algorithm
<input checked="" type="checkbox"/>	Inter-function forgery detection code
<input checked="" type="checkbox"/>	Hash algorithm
<input checked="" type="checkbox"/>	String encryption
<input checked="" type="checkbox"/>	Constant encryption
<input checked="" type="checkbox"/>	Dummy code



### Key Functions

(Functions provided by the script with Dynamic Change Factor applied)

- HTML forgery prevention and obfuscation.
- URL de-identification.
- JavaScript obfuscation.
- Developer tool detection.
- Operation data encryption (E2E)
- Scrapping prevention
- Session forgery detection/blocking

(\*) Dynamic Change Factors : Security script is running by changing the factors indicated in the table everyday or by certain cycle.

- Toss Bank, indiscriminately collects the **Credit Card Loan User's Information of Samsung Card** through Web Scrapping method.



### Background of Adoption in Samsung Card

Toss Bank, expanding to the Credit Card Companies subject to Replacement Loan of Credit Card Loans

이 서비스는 토스뱅크가 중저신용자 신용대출 비중을 끌어올리는 데도 도움이 될 전망이다. 토스뱅크는 올해 연말까지 중저신용자 신용대출 비중을 42%까지 높이겠다는 계획을 금융당국에 제출했다. 지난 3월 말 기준 이 비중은 31.4%였다.

카드사들은 기존 고객의 이탈이 우려돼 반발하고 있다.

카드업계에서는 토스뱅크가 카드론 정보를 수집하는 과정에서 사용하는 '웹 스크래핑' 방식이 보안상 취약할 수 있다는 점 등을 문제 삼고 있다.

The credit card industry is calling into question about the possible security vulnerability of the 'Web Scrapping' method used by Toss Bank in the middle of collecting Credit Card Loan information.

같은 은행권에서도 토스뱅크의 이런 서비스는 다소 파격적이라는 평이 나온다.

은행권의 한 관계자는 "보수적인 기성 은행권에서는 고려하기 어려운 서비스"라며 "특히 다른 사업에서의 카드사와의 제휴 관계 등을 고려하면 시도하기 어렵다"고 말했다.



**Unauthorized collection of Credit Card Loan information** without the consent of holder or manager of the data.



**Unclear Responsibility** in case of any accident as personal information leakage by scrapping, etc.



**Lack of Legal and Institutional Measures to Regulate** the companies which are not My Data Operators

➤ Results of Application of Eversafe for Web (Continued)

### Samsung Card Before Using Solution

As-Is Attempted scrapping by analyzing the static E2E data

```
POST http://192.168.0.240:8080/apply/SvcLogin.pwkison?hospitalCd=321321 HTTP/1.1
Host: 192.168.0.240:8080
Connection: keep-alive
Content-Length: 857
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.0.240:8080
Referer: http://192.168.0.240:8080/apply/dynamic
Accept-Encoding: gzip, deflate
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7,und;q=0.6
Cookie: JSESSIONID=5B62DDC99921328D3321AE8C724C768F; lang=ko; bodyYn=Y
{"loginFrmVo":{"authType":"01","userId":"admin","loginGubun":"01","birth":"","userPwd":"admin@12","
```

- As the E2E does not change and is composed statically, it allows the web scrapping
  - ⇒ Can be bypassed by analyzing static E2E data

### Samsung Card After Using Solution

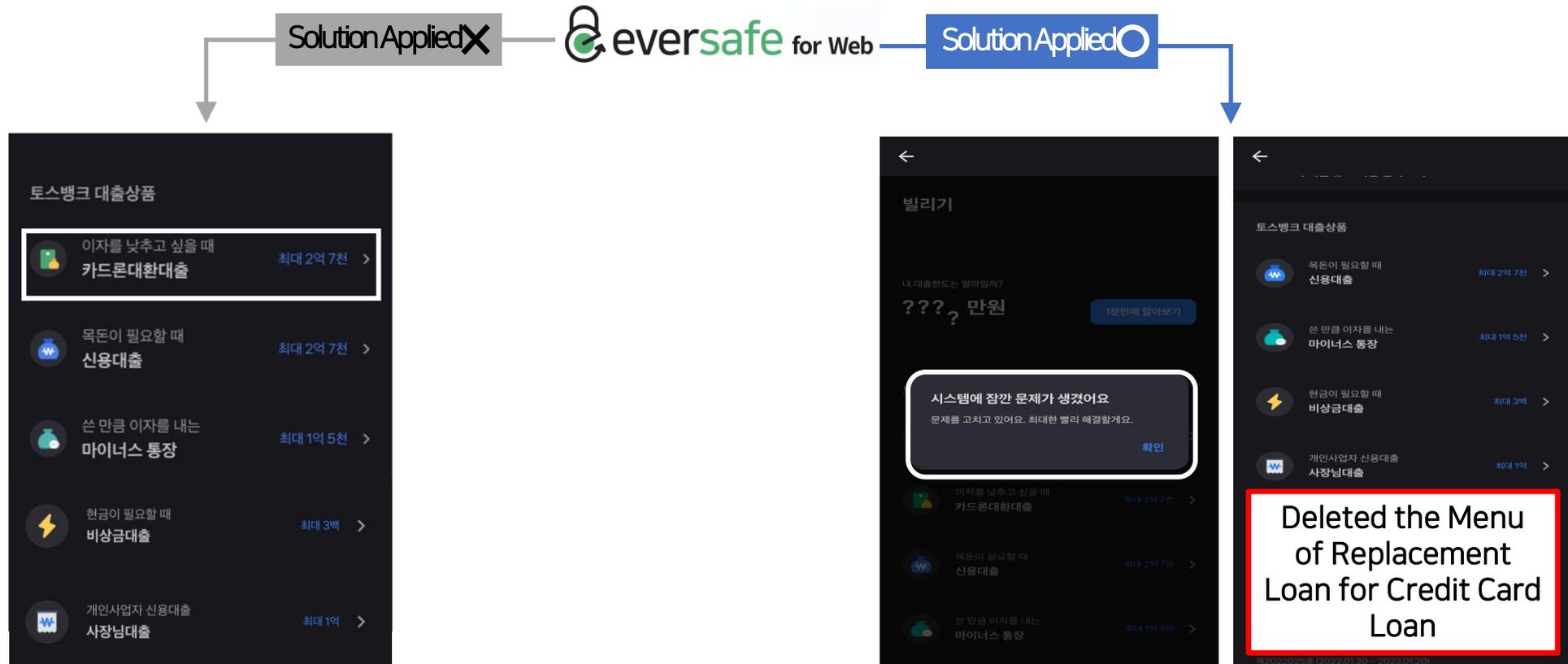
To-Be Dynamic-based E2E data

```
{ "z16Hbr": "Znq5zLpCunc9C7KeN7KnuLT8J01jtMqfzLW1uIC1u641p6CluIqoQhtwzblAjcKnu7KXncKnuIXTqiCnqi5qiCf"
{ "JUNGdA": "5eVTSwZuIOaMaOUjGOUeyfgKPEN7FOV45f6NybaNyRuN9RAnybVZ2tFrSDNcPxUey0UCGxUeybyGVAaeVAVHVAae"
⋮
{ "n6FRId": "uc86uecnp1r0rbwZvbWCpGV0xDeo1286tgSePirePaResarePi83J917tNeQxZWCpWUvzWCPiyV8prC8p8K8prC
```

- As the encryption code, algorithm and key, etc. are changed by certain cycle, the web scrapping is COMPLETELY BLOCKED
  - ⇒ Analyzing itself is difficult as all location, storage method, etc. are changed variably.

➤ Results of Application of Eversafe for Web (Continued)

- After using the EverSafe for Web, the **Toss service Suspended Replacement Loan for Credit Card Loan targeting Samsung Card**



Activation of Replacement Loan for Credit Card Loans Through Scrapping

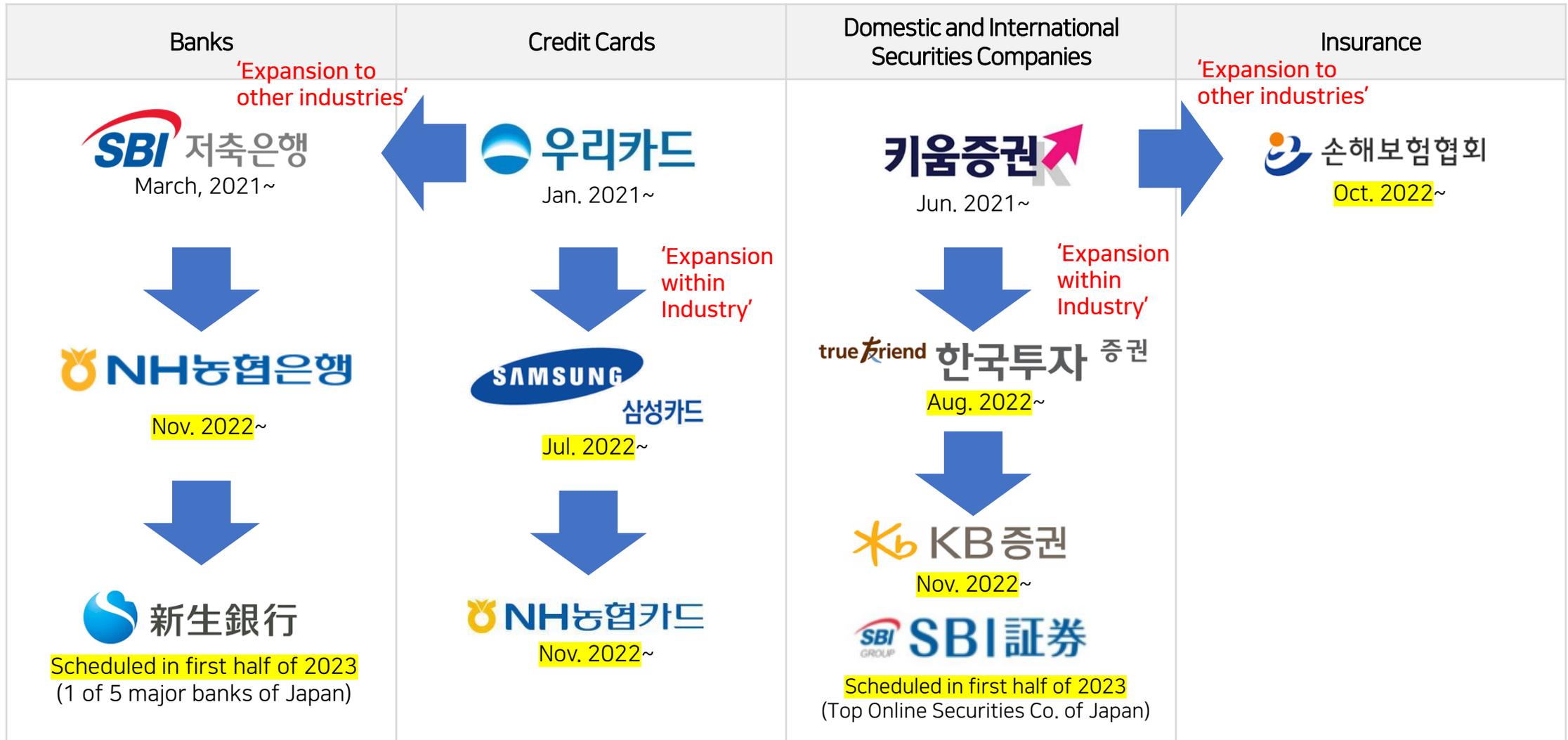
By Complete Blocking of Scrapping, Suspended the Replacement Loan Service for Credit Card Loans

## ➤ Results of Application of Eversafe for Web (Continued)

- Even after the suspension of replacement loan service for credit card loans by Toss, **there are still performed continuous attempts to hack and bypass the EVERSPIN security module to attempt the act of scrapping.**
- Everyday, **diverse attacks are attempted** to bypass the Eversafe for Web but, **they are always Blocked Completely by the Moving Target Defense-based security script as follows.**

Classification	No. of E2E threat occurrence	No. of detections suspected as Toss	E2E Threat Occurrence / Toss suspected detection rate	Reason
2022-07-06	1007	930	92.35%	1. Scraping flag detect 2. Param name notmatch 3. Empty body 4. Not exists referrer 5. MITM refer( <a href="http://40.225.192.36/">http://40.225.192.36/</a> ) 6. Autobot(168.126.153.*, 210.123.95.*)
2022-07-07	1259	1210	96.11%	
2022-07-08	860	811	94.30%	
2022-07-09	733	710	96.86%	
2022-07-10	849	834	98.23%	
2022-07-11	796	711	89.32%	
2022-07-12	762	721	94.62%	
2022-07-13	1059	717	67.71%	
2022-07-14	5207	5186	99.60%	
2022-07-15	1134	1105	97.44%	
2022-07-16	858	845	98.48%	
2022-07-17	791	771	97.47%	
2022-07-18	802	742	92.52%	
2022-07-19	758	731	96.44%	
2022-07-20	780	736	94.36%	
Daily Average	1177	1117	93.72%	

- Currently, EverSafe for WEB, has proved the technological effectiveness in all industries of bank, credit card, securities, insurance, etc. since its Initial launching in 2021. It became the Next Generation Web Anti-Hacking Security Solution which secured Major References in all Industries by winning-back the limitations of conventional solutions with predominant technology



(2) Anti-Phishing Solution



World's First Whitelist (True Apps List)-based Technology

- ✓ Known Malicious Apps = Apps which already caused damages

The currently existing malicious app detection solution can detect and block malicious apps as a post-treatment which registers the malicious apps when the respective app is well known by already causing critical incidents.

→ Thus, the current technology has the limitation that cannot detect and block malicious apps before incident occurs.

Known Malicious Apps



VS

Unknown Malicious Apps



## Fake App

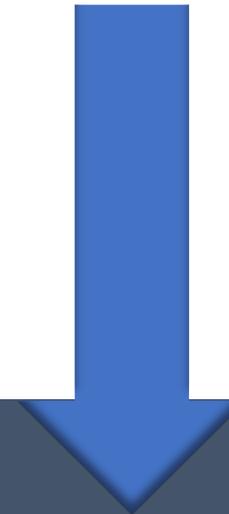
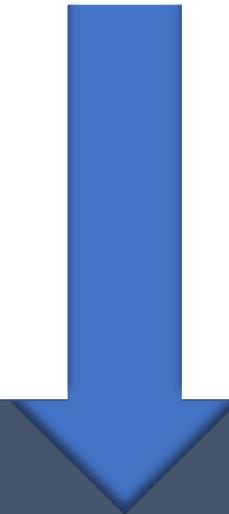
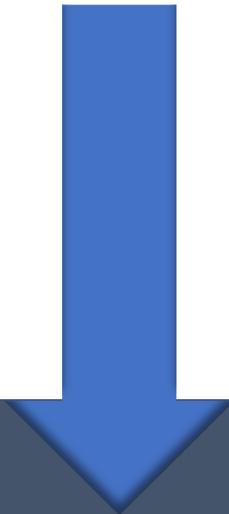
(ex. Disguised app, misrepresenting app, voice phishing app)

## Malware App

(ex. Diverse apps with purpose to steal personal information of users)

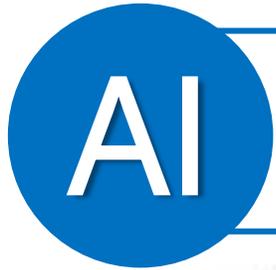
## Forged App

(ex. App which was forged and altered from normally distributed apps)

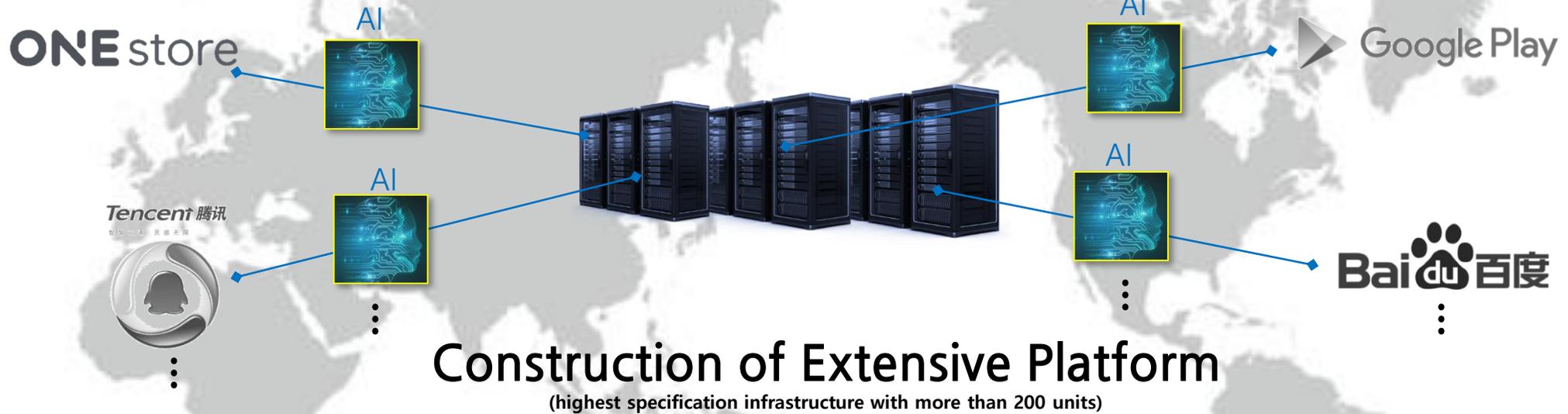


**Most of the malicious apps of the world  
are not distributed through official markets**

(Common characteristics of most of the malicious apps)



Robot collects all true apps from all official stores around the world in real-time



### Construction of Extensive Platform

(highest specification infrastructure with more than 200 units)

Human cannot gather it

- ✓ There are hundreds of Google Play Stores (by country ... )
- ✓ Too many private markets (T-store, Baidu market, Tencent market ... )
- ✓ Only the number of apps which were distributed via official markets is more than 19 million.

## Extensive BIG DATA collected throughout 4 years

In May, 2023 (excluded number of overlapped Apps by country/market)

Number  
of collected apps

**19,964** thousand apps

Total volume  
of collected apps

**230** TB

Fake Finder has been proved to be the **ONLY TECHNOLOGY** to detect and block all malicious apps **in advance** among all currently existing Anti-Phishing Technologies.

Detected time	STATUS	PACKAGE_ID	PACKAGE_NAME
2022-05-31 16:45:41	DANGER (10001)	netne.ono.ce	CJ대한통운 택배.
2022-05-31 16:37:48	DANGER (10003)	com.fbnk.nonghep	NH농협은행
2022-05-31 16:36:07	DANGER (10003)	com.fbnk.kakao	카카오뱅크
2022-05-31 16:35:31	DANGER (10001)	com.dsbewjfquujf9ewj.security	보안프로그램
2022-05-31 16:34:32	DANGER (10003)	com.parallel.space.lite.arm64	Parallel Space Lite 64Bit Support
2022-05-31 16:33:14	DANGER (10001)	com.dsbdswjguye8ewj.security	보안프로그램
2022-05-31 16:31:47	DANGER (10001)	com.dsbdsfjuq22jdnq.security	보안프로그램
2022-05-31 16:28:09	DANGER (10001)	com.dsbwejfjuewd29hhhe.security	보안프로그램
2022-05-31 16:25:08	DANGER (10001)	com.yjdlsoft.mtrsv	금융보안프로그램
2022-05-31 16:20:45	DANGER (10003)	com.fbnk.shinhan	신한은행
2022-05-31 16:19:05	DANGER (10001)	com.app.main	금융보안프로그램
2022-05-31 16:19:05	DANGER (10003)	com.app.web	OK저축
2022-05-31 16:15:00	DANGER (10001)	com.dsbdeghuwh6ewh.security	보안프로그램

**1 Reliability of Detection Outcomes**

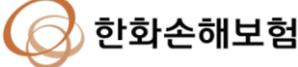
- **DAU(daily active user): over 14 mill.**
- **Accumulated no. of preventive detection : 573,916 cases** (735 days, Oct 2020~Oct 2022)
- **DATA reliability: 100% scouted** (checked by client)

**2 Unique method blocking in advance**

Most of the malicious apps are distributed spontaneously.

Even the same malicious app is distributed with partial changes. As most of the malicious apps are not reused, the method to prevent reoccurrence based on blacklist is practically useless

- In only 2 years (released in Oct. 2020) from release, secured 44 major clients in and outside Korea (42 in Korea, 2 overseas)
- Fake Finder is the practically Only Solution which can resolve the social issue of phishing, and it has been proved through best performances and results.

Bank	Credit card, capital	Savings bank	Insurance companies	Domestic-international securities companies
6 sites in Bank	6 sites in Credit Card Co.	13 sites of Savings Bank	7 sites of Insurance Co.	6 domestic sites
 KB 국민은행  NH농협은행  kakaobank  Kbank  BNK 부산은행  BNK 경남은행	 Hyundai Card  KB 국민카드  SAMSUNG CARD  우리나라 우리카드  LOTTE CARD  NH농협카드  4sites of Capital Co.  Hyundai Capital  BNK 캐피탈  true friend 한국투자 캐피탈  finda	 웰컴저축은행  SBI 저축은행  예가람저축은행  true friend 한국투자 저축은행  SB 저축은행중앙회  고려저축은행  ES저축은행  애큐온저축은행  DAOL 다올저축은행  JT 저축은행  모아저축은행  진주저축은행  pepper 페퍼저축은행	 삼성생명 SAMSUNG  SAMSUNG 삼성화재  한화생명  한화손해보험  신한생명  MIRAE ASSET 미래에셋생명  KYOBO 교보생명	 true friend 한국투자 증권  신한금융투자  하나증권  KB 증권  EBEST 이베스트투자증권  현대차증권  2 overseas sites  SBI証券  SBI GROUP 新生銀行

### 3 Technology

has been fully **proven** globally

# 6. What is the theoretical basis of Eversafe?

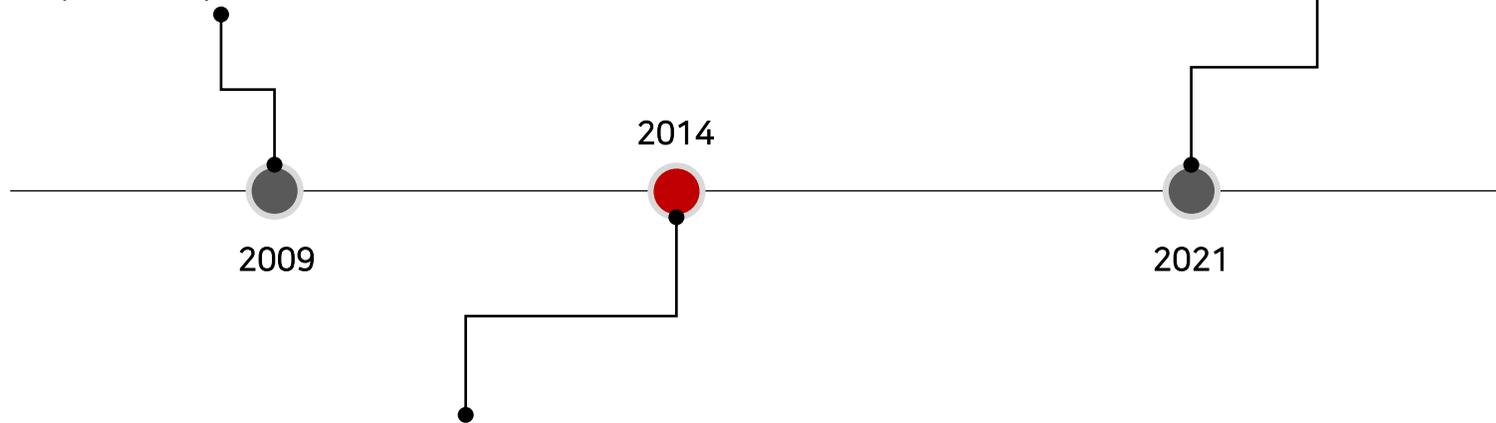
Everspin commercialized concept **MTD(moving target defense)** which was created **by the Obama administration in 2009** and was highlighted **by Gartner in 2021**.



**Obama Administration of U.S.** defined MTD(Moving Target Defense) as a top out of 5 game changing initiatives in cybersecurity industry (National Cyber Leap Year Summit, 2009)



**Gartner** issued critical insights on MTD(\*) for app security as an emerging technology



**Everspin** started commercializing MTD concept by providing anti-hacking solution with dynamic technology to top financial institutions, even if other competitors are just at the stage of R&D.

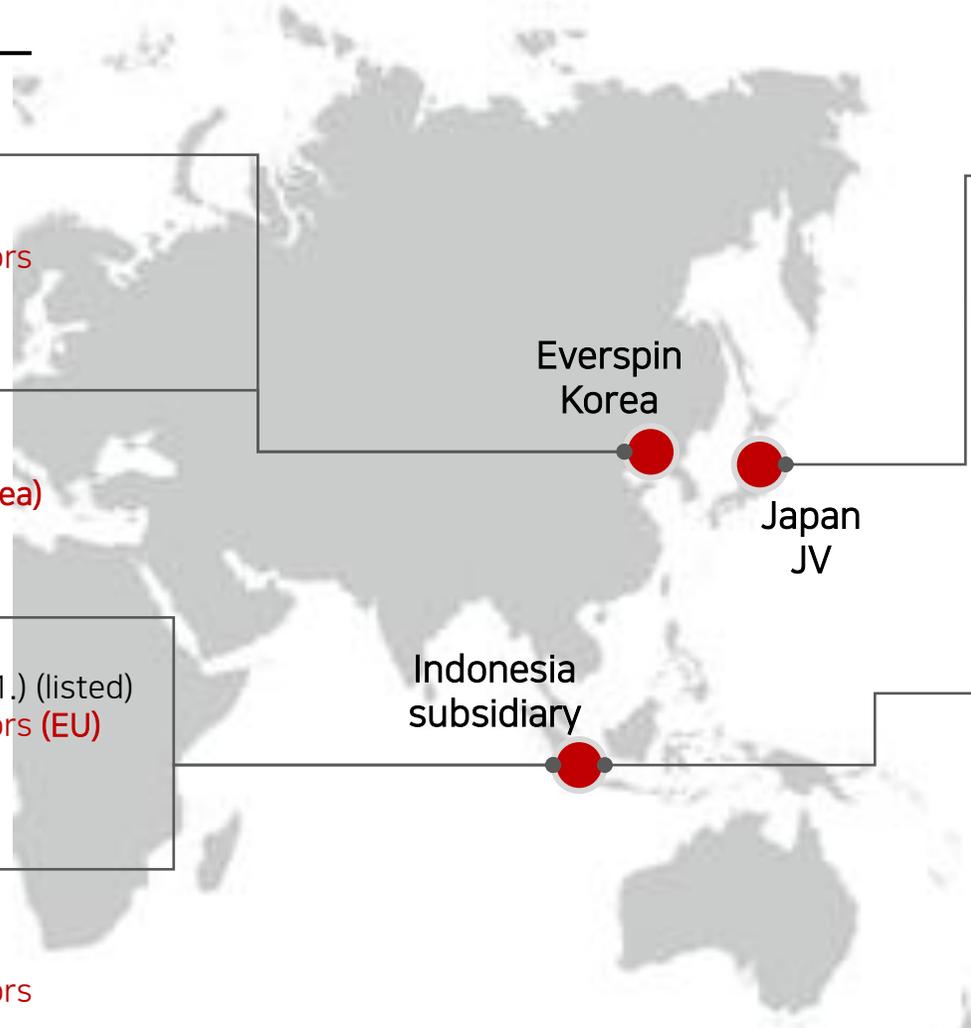
(\*) Assume an expert thief is able to pick the lock to any door. The goal of MTD is not to build a better lock. Instead, the goal of an MTD security strategy is to make the door and the door's lock difficult or impossible for the thief to find.

# 7. How effective is Eversafe?

Our solution won all BMTs against U.S. & E.U. vendors and passed the 3<sup>rd</sup> party pen-tests successfully.

## Won BMT (benchmark test)

- 
  - 3<sup>rd</sup> largest Bank (listed)
  - Won against 7 global vendors (US, Korea)
- 
  - 1st largest Bank
  - Won against 2 vendors (Korea)
- 
  - 3<sup>rd</sup> largest Bank (Online No1.) (listed)
  - Won against 1 global vendors (EU)
- 
  - 4<sup>th</sup> largest Bank (listed)
  - Won against 2 global vendors (US, EU)



## Passed 3<sup>rd</sup> party pen-test

### Deloitte.

- Penetrating test for SBI Group
- Result: Pass (2019)

Checklist items	Status
Successfully making a modified/forged application and performing a log-in on the modified/forged application	Unachieved
Time of the successful login	Unachieved
Username(s) that were able to successfully login	Unachieved
Run the modified/forged application on a non-rooted device or unmodified OS	Unachieved
Repeated successful login with modified/forged application	Unachieved

### ITSEC<sup>TM</sup> SECURITY DELIVERED

- Penetrating test for Mandiri Bank
- Result: Pass (2020)
- Detail: No findings based on risk categories as extreme and high.

# 8. How effective is FakeFinder?

Our solution is more faithful to cybersecurity principle in that **even unknown malicious apps** are detected **in advance**.

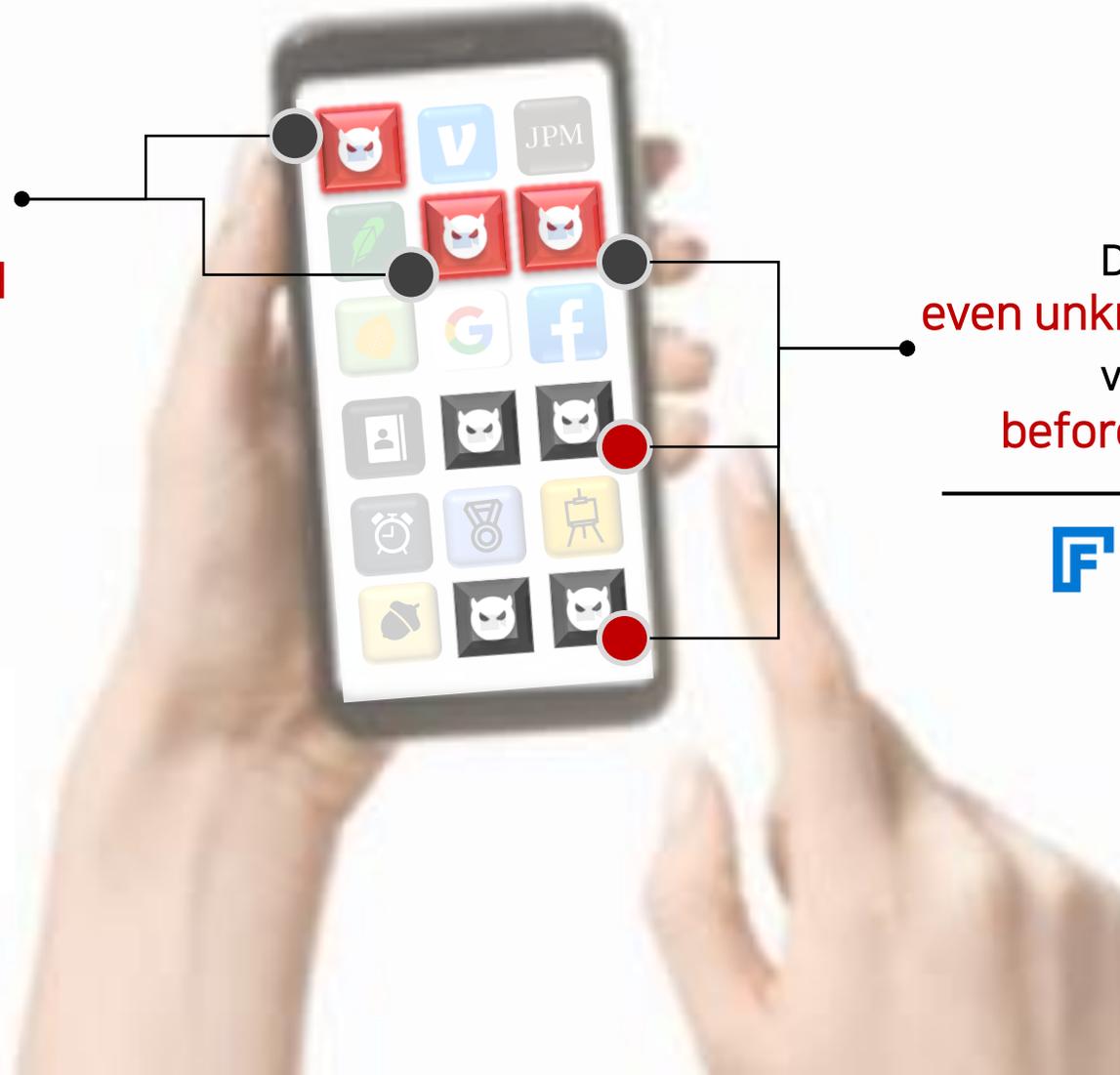
Detect & block **known malicious apps** via Blacklist **only after incidents occurred**



Avira Avast Kaspersky



Norton McAfee ESET



Detect & block **even unknown malicious apps** via Whitelist **before incidents occur**

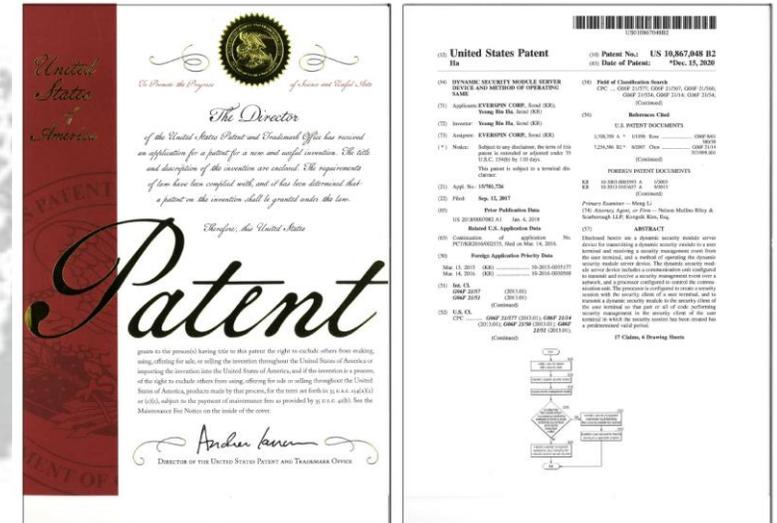


# 9. How is our technology protected?

Three patents were registered in 11 countries.



[Example in the U.S.]



**US 10,867,048 B2**  
 Dynamic Security Module Server Device and Method of Operating Same(15 Dec 2020)

**US 10,867,049 B2**  
 Dynamic Security Module Terminal Device and Method of Operating Same (15 Dec 2020)

**US 10,867,050 B2**  
 Method and apparatus for generating Dynamic Secure Module(15 Dec 2020)

# 10. How well has been Everspin recognized?

Everspin has won many awards & prizes all over the world, was appointed as a unique cybersecurity company to visit U.S. together with a Korean President in 2023.

- Won 1<sup>st</sup> Prize in tryout of Korea
- ARCH Summit 2020 in 2019
- Final was cancelled due to Covid19

Luxembourg

Switzerland

- Won 1<sup>st</sup> Prize
- Swiss Post Innovation Pitch Contest in 2017 held by Switzerland Post

Korea

- Won President's Award(1<sup>st</sup> Prize)
- K-Startup Grand Challenge in 2017
- Nation-wide startup program held by Korean Government
- Good Software Certificate(\*) as a vendor to government

Japan

- Won Prize as a Korean company first
- FIBC Fintech Contest in 2016
- Japan's Largest Fintech conference held by the top Japanese banks

Singapore

- Won 1<sup>st</sup> Prize
- Singapore Fintech Festival in 2018
- Asia's Largest Fintech Award Festival held by the top banks and the Monetary Authority in Singapore

U.S.



- Was appointed as Korean economy delegation to U.S. in April of 2023
- Unique cybersecurity company out of 122 Korean companies for visiting U.S. with Korean President
- IR to 39 venture capitals in U.S. during Korea-U.S. Cluster Round Table

(\*) GS Certificate



## **4** Business feasibility

has been fully **proven** in Korea

# 11. How is market dominance in Korea?

Everspin has been focusing on top financial institution at first **strategically** and expanding now, so **40M people out of 51M Korean population** are protected by our solutions.

## Korea

## APAC

5/top 6

6/top 9

6/top 8

7/top 8

6/top 8

'Industry'  
expansion

Rank(*)	Banks	Securities	Credit Cards	Saving Banks	Insurances
1st	KOOKMIN	MIRAE ASSET	SHINHAN	SBI	SAMSUNG
2nd	SHINHAN	KOREA INVST	KOOKMIN	OK	HANWHA LIFE
3rd	KEB HANA	NH	SAMSUNG	KOREA INVST	KYOBO LIFE
4th	WOORI	SAMSUNG	HYUNDAI	WELCOME	NH
5th	IBK	KOOKMIN	LOTTE	PEPPER	MIRAE ASSET
6th	NH	MERITZ	WOORI	ACUON	HANWHA
7th	BNK	HANA	HANA	DAOL	SHINHAN
8th		SHINHAN	NH	MOA	KYOBO
9th		KIWOOM			



Fin-Techs
KAKAO Bank
K-BANK
FINDA



'Market'  
expansion

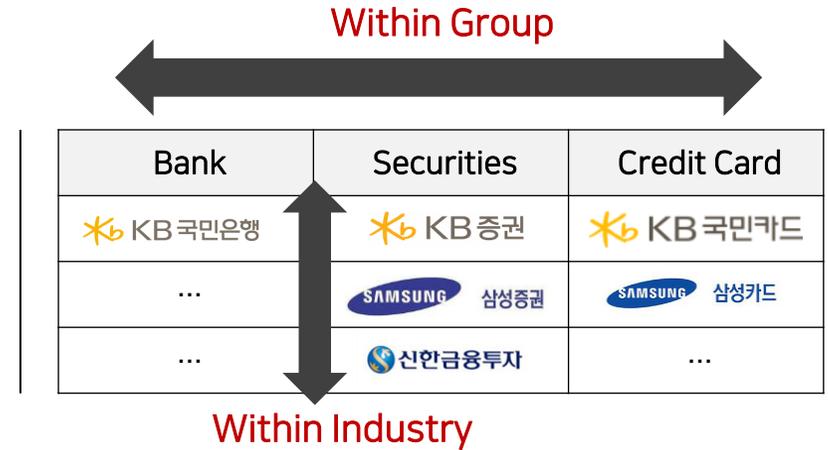
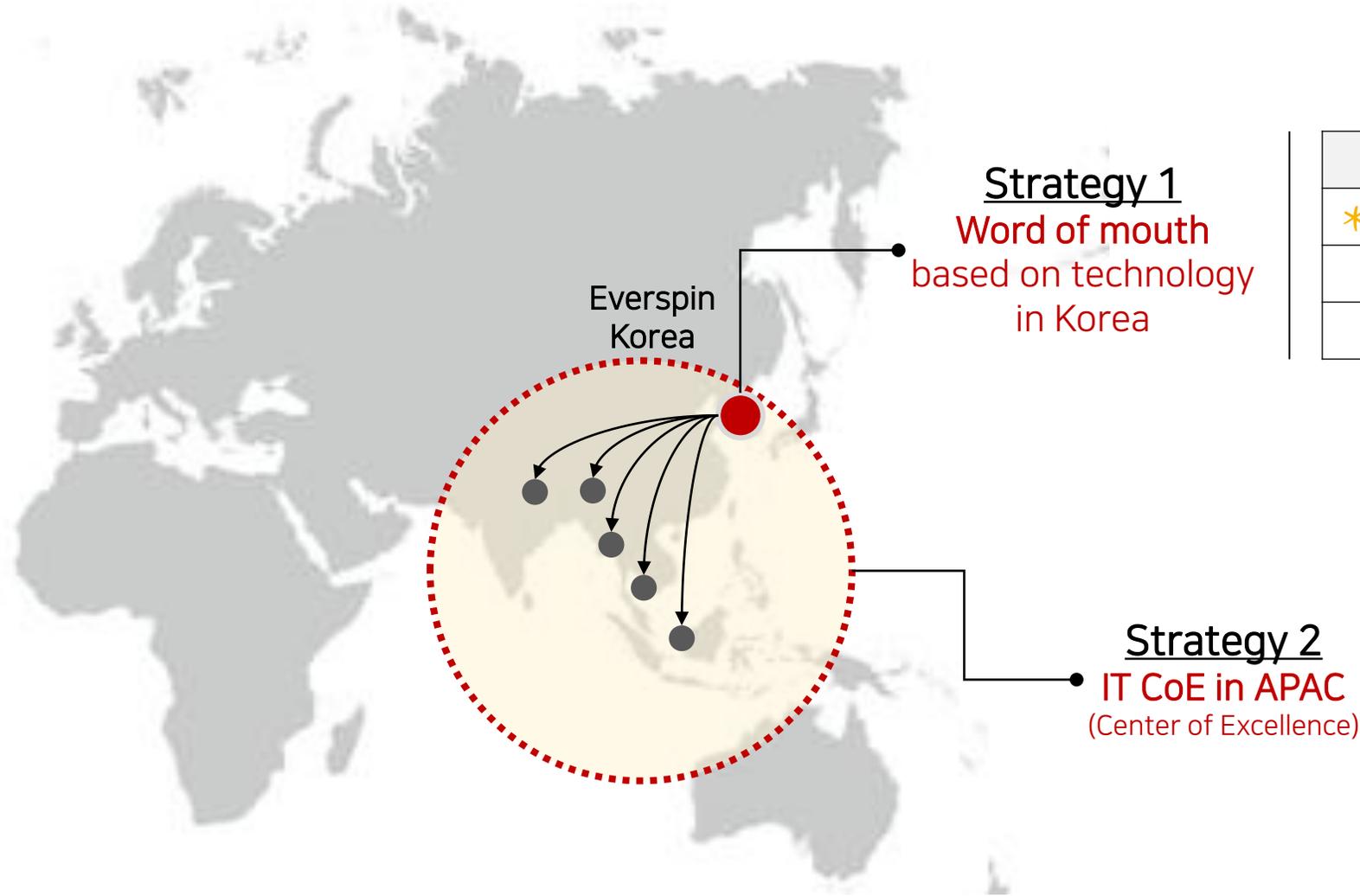
4 Banks/Securities
SBI Securities(JP)
SHINSEI Bank(JP)
MANDIRI Bank(IND)
JAGO Bank(IND)

(\*) Ranking based on total asset or revenue or number of customer in Korea

**5** Our solutions  
are getting required to solve  
**common problems**  
in every sector all over the world

# 12. How has been global expansion so far?

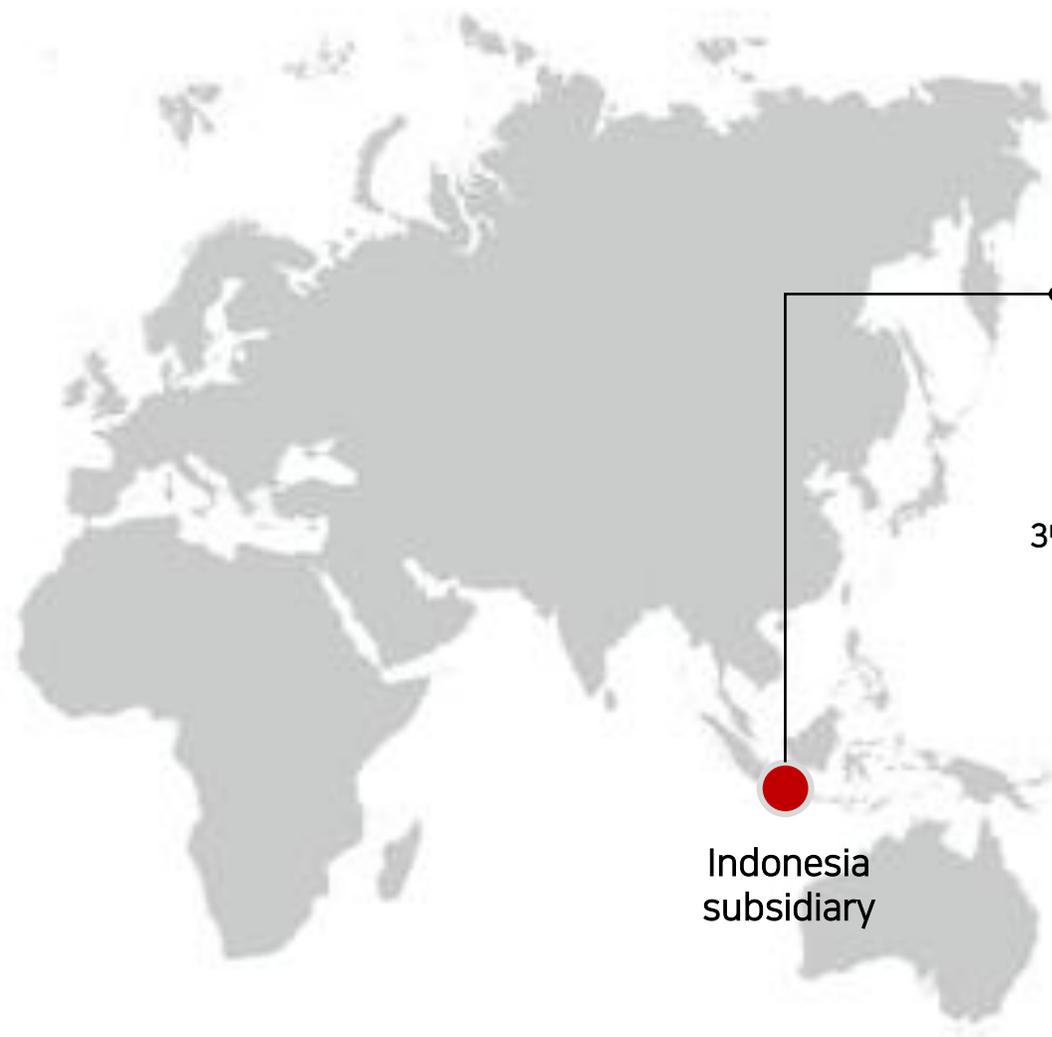
## (1) Korea



- Korean financial institutions has entered APAC market by **establishing or acquiring** local companies.
- Market dominance in Korea means that Everspin can dominate APAC market by setting up manpower and sales forces based on competitive technology

# 13. How has been global expansion so far?

## (2) Indonesia subsidiary



### Strategy 1

**Top Reference First**  
(As a Joint Venture until 2022)



3<sup>rd</sup> largest Bank (Online No1.) (listed)



4<sup>th</sup> largest Bank (listed)



Other Local  
Financial Institutions



### Strategy 2

**Korean Reference Based**  
(As a Subsidiary from 2023)

Current References in Korea



Other Local Financial  
Institutions that Korean  
companies acquired

# 14. How has been global expansion so far?

## (3) Japan JV

**Strategy 1**  
Group Reference First  
(So far)

**SBI証券**  
No1. Securities (listed)

**SBI 新生銀行**  
No7. Bank (listed)



Group Companies

Japan JV

**Strategy 2**

via National Police Agency  
(From now on)

- JC3(\*1) is like NCFTA(\*2) in U.S.
- Joined JC3 as a regular member, which means Everspin's solution is considered as a **standard solution** to deal with cybersecurity issues in Japan.
- SBI group(4 companies) plans to do co-marketing on Eversafe & FakeFinder with JC3 in 2023.

(\*1) [Japan Cybercrime Control Center](#)

(\*2) [National Cyber-Forensics and Training Alliance](#)



正会員			
Afiac	<b>SBI EVERSPIN</b>	SBI 新生銀行	SBI Holdings
SBI証券	NTT	NTT Data	NTT Data
NTT	JTB	SECOM	SECOM
Z HOLDINGS	YAHOO!	LINE	LINE Pay
Selliton	Deloitte	TREND	NEC
IBM	HITACHI	bitflyer	FUJITSU
MIZUHO	SMBC	日本銀行	SMBC 三井住友銀行
MUFG	mercari	merpay	ゆうちょ銀行

## 6 Success Stories in Indonesia (EVERSPIN Indonesia)

Everspin Indonesia which was established in 2019 is well localized enough to provide close technical support to Indonesian customers directly, which has been proven by Bank Jago, a top-class bank in Indonesia.

