

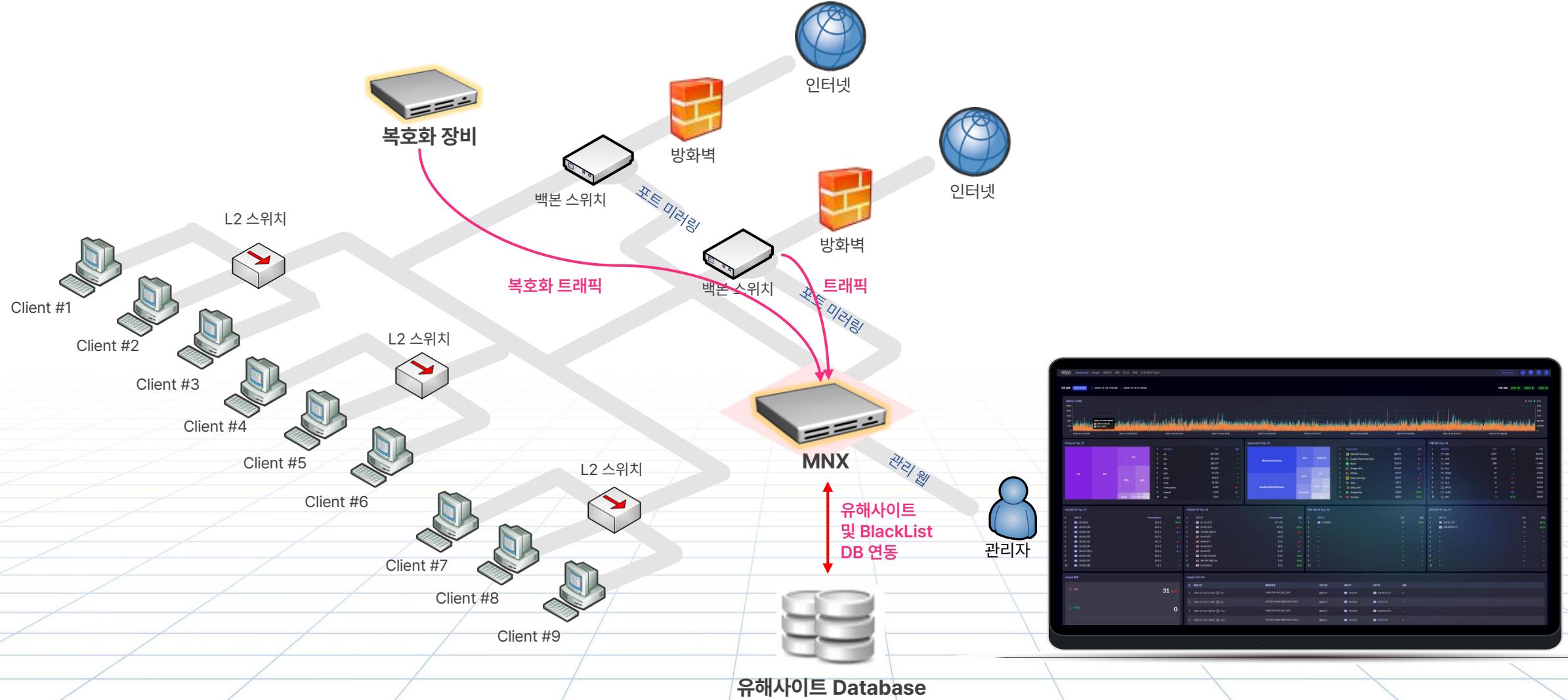
# THE #1 MNX DPI 제품 / 아키텍처 소개 자료

개요

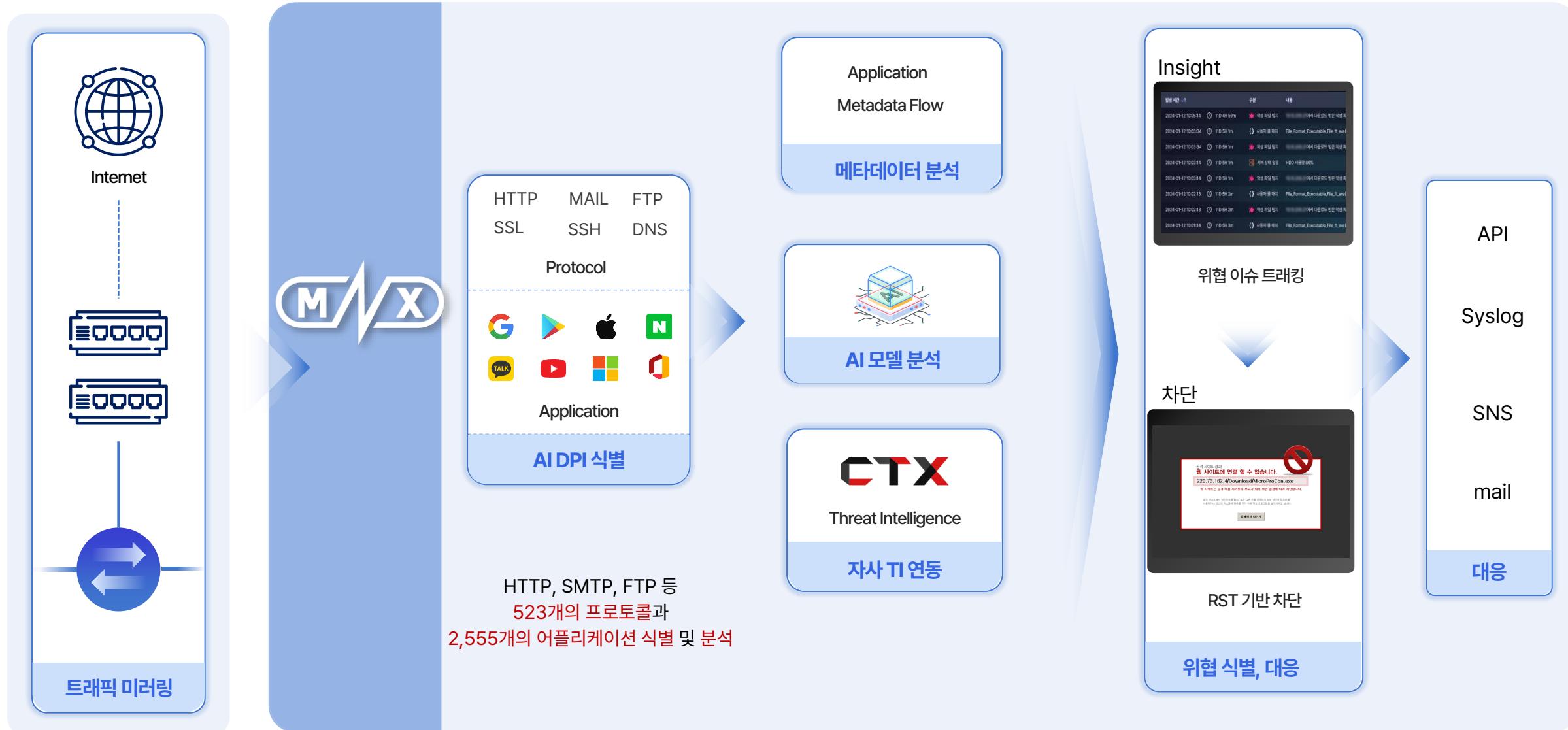


# 1. 구성도

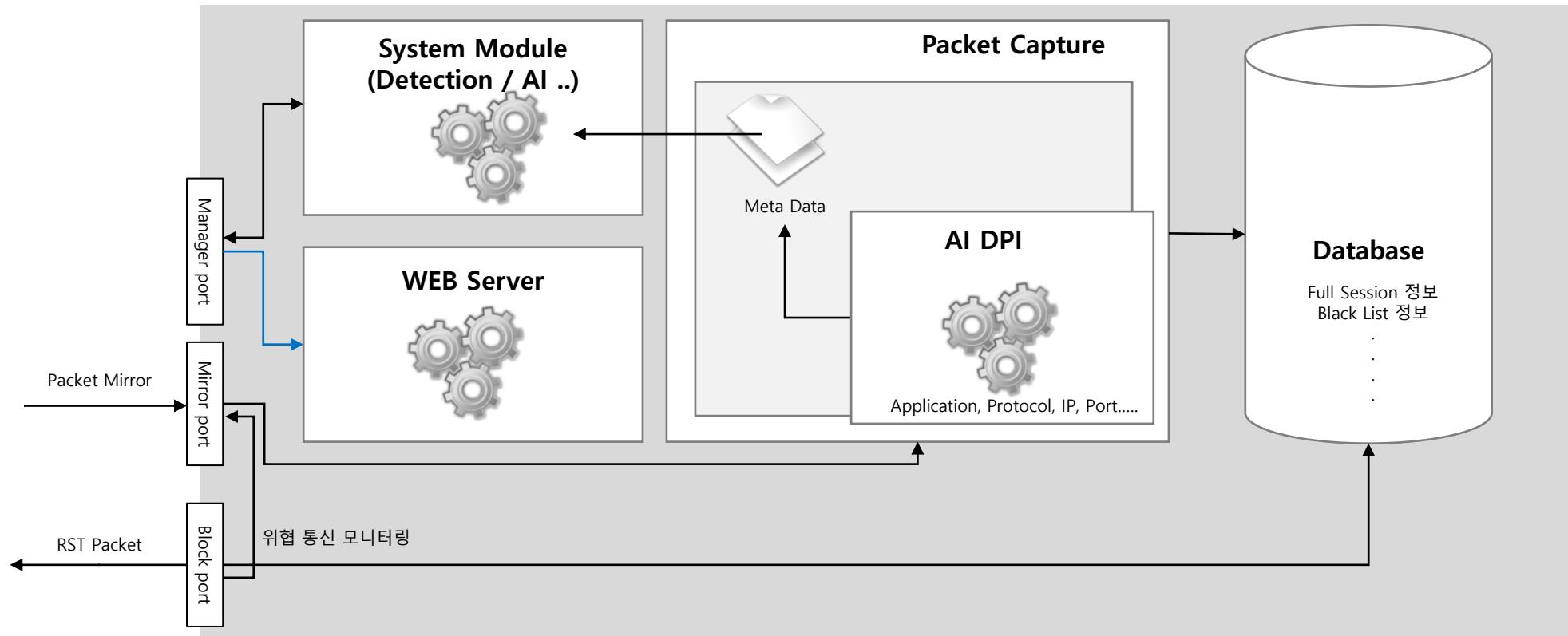
## - Mirror 방식 구성



## 2. 시스템 구성도



### 3. 시스템 아키텍처



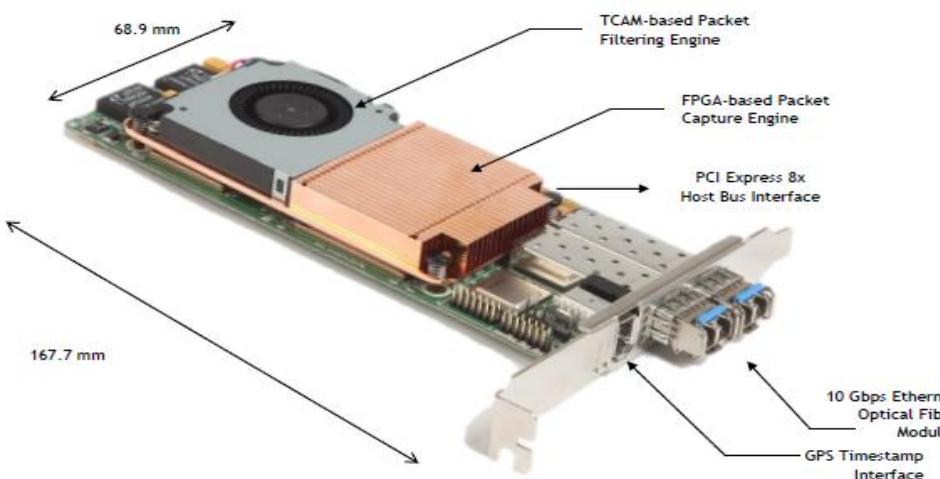
\* 공개 가능 일부 부분

기능

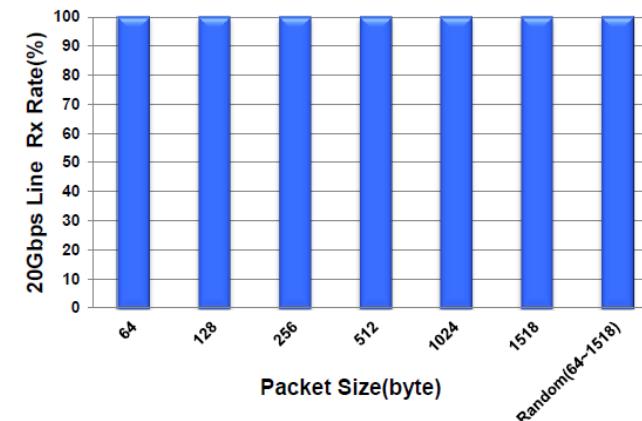


# 1. 수집

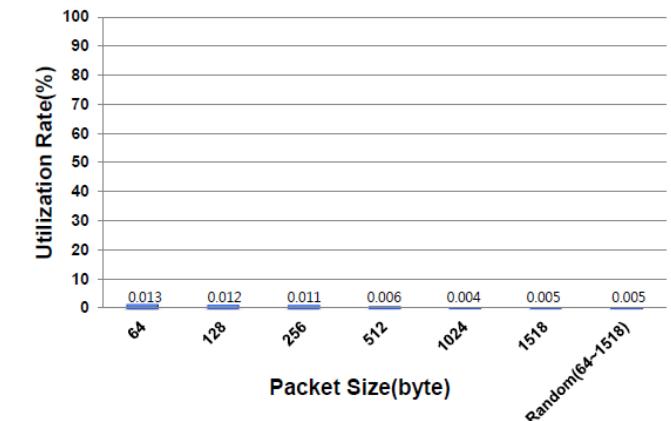
## - 수집 전용 Network 카드



■ Capture Processing Performance(%)

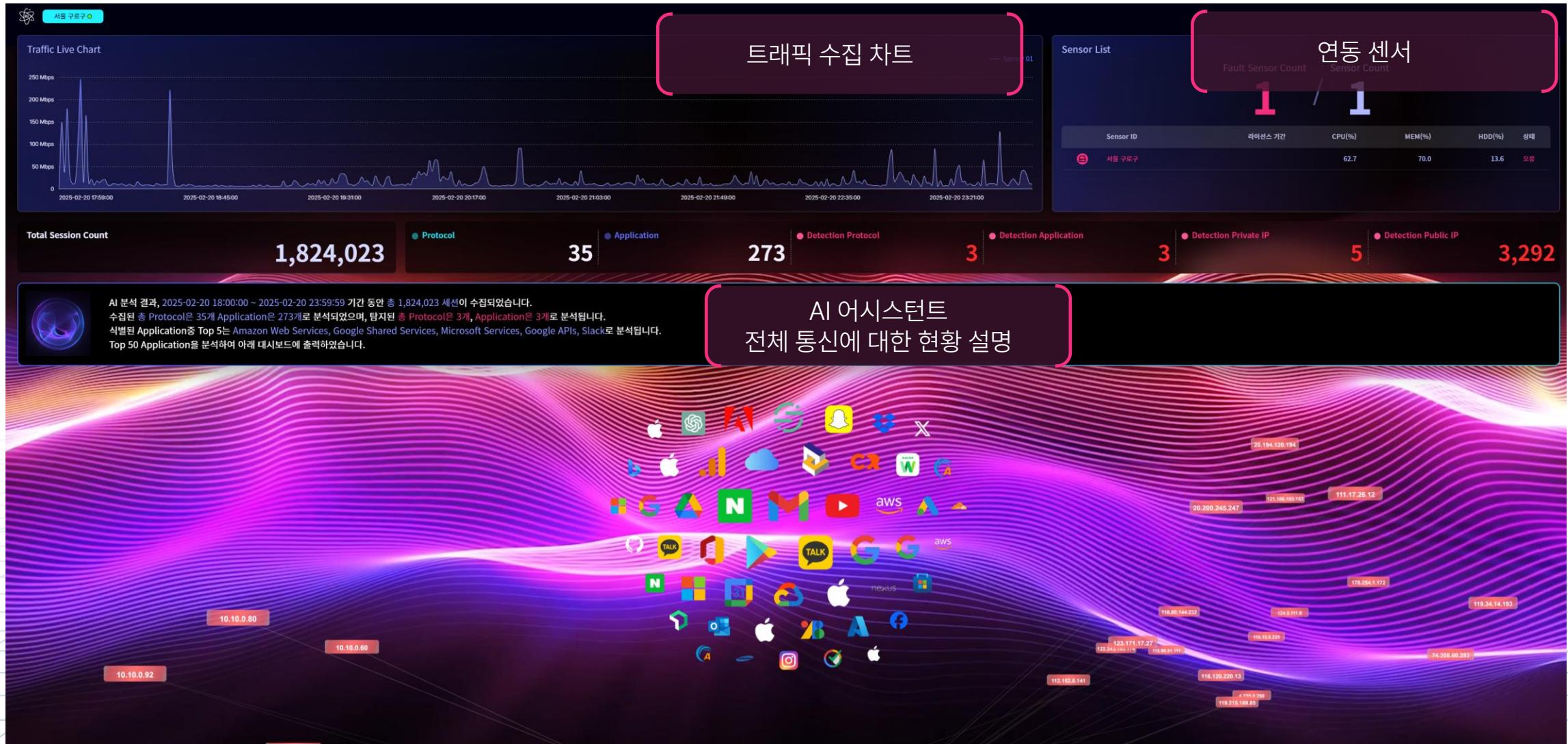


■ CPU utilization(%)



각종 신호를 H/W 레벨에서 처리하여 Packet 손실 0%로 제공. 10Gbps 대역대 무손실 수집 지원

## 1. 수집 - WEB



## 2. AI DPI 분석

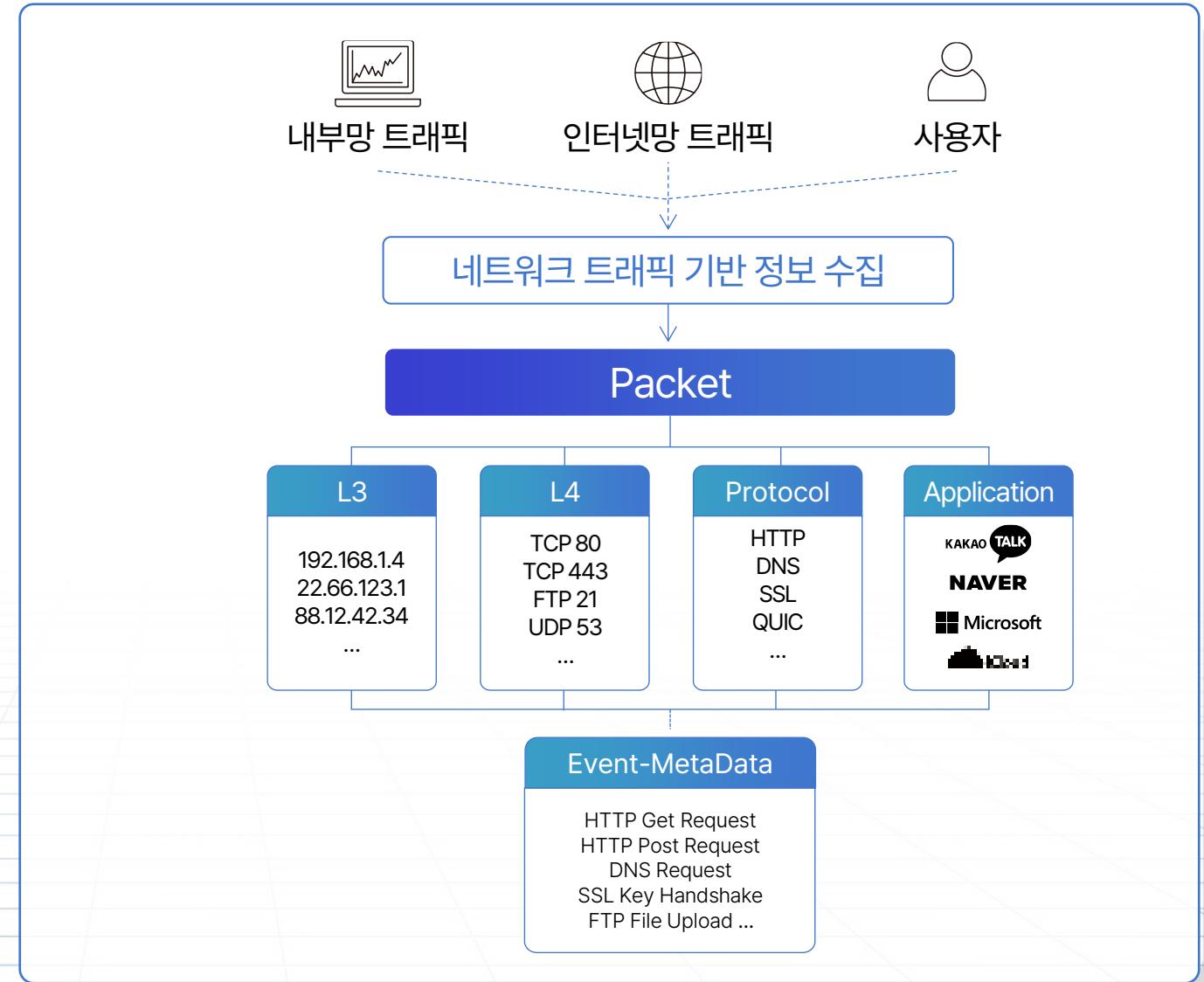
### - AI DPI 개요

#### AI 기반

#### DPI(Depth Packet Inspection)을 통한 가시성 확보와 상세한 메타데이터 추출 및 분석

네트워크 레이어의 최상위에 있는  
L7 패킷 전체에 대한 검사를 수행,  
500종 이상의 L7 프로토콜을 식별

세션 별 SRC IP, DST IP, Protocol,  
Application 정보를 제공하여 상세한  
트래픽 정보를 확인

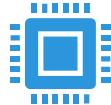


## 2. AI DPI 분석

### - AI DPI 학습 모델

```
monday.pcap.summary x
:1,"send_hdr_len":132,"recv_hdr_len":66,"protocol": {"id":26
4,"name": "OCSP"}, "application": {"id":0,"name": "n/a"}, "tcp_session": "not-finished"
816971
{"flow_id":3447639296,"start_ts":1499112094352,"end_ts":14991
12094413,"network_packet_feature": {"fl_dur":61,"src_ip": "192.
168.10.3","src_port":61086,"dst_ip": "192.168.10.1","dst_port"
:53,"tot_all_pkt":2,"tot_all_pkt_size":265,"tot_send_pkt":1,"tot_
send_pkt_size":159,"tot_recv_pkt":1,"tot_recv_pkt_size":106,"send_
pkt_max_size":159,"send_pkt_min_size":159,"send_pkt_avg_size":159,
"send_pkt_std_size":0,"recv_pkt_max_size":106,"recv_pkt_std_
size":0,"fl_byt_s":265,"fl_pkt_s":2,"fl_iat_avg":61,"fl_iat_s
td":0,"fl_iat_max":61,"fl_iat_min":61,"send_iat_tot":0,"send_
iat_avg":0,"send_iat_std":0,"send_iat_max":0,"send_iat_min":0,
"recv_iat_tot":0,"recv_iat_avg":0,"recv_iat_std":0,"recv_iat_
max":0,"recv_iat_min":0,"send_pkt_s":1,"recv_pkt_s":1,"pkt_l
en_min":106,"pkt_len_max":159,"pkt_len_avg":132.5,"pkt_len_st
d":26.5,"send_psh_flag":0,"recv_psh_flag":0,"send_urg_flag":0,
"recv_urg_flag":0,"fin_cnt":0,"syn_cnt":0,"rst_cnt":0,"psh_c
nt":0,"ack_cnt":0,"urg_cnt":0,"ece_cnt":0,"cwr_cnt":0,"send_
seg_avg":0,"send_seg_min":0,"recv_seg_avg":0,"send_win_byt":0,
"recv_win_byt":0,"send_act_pkt":0,"send_hdr_len":42,"recv_hdr_
len":42,"protocol": {"id": 1,"name": "TCP"}, "application": {"id": 1,
"name": "Google Shared Services"}, "tcp_session": "not-finished"
816972
{"flow_id":3447640064,"start_ts":1499112094352,"end_ts":14991
12094413,"network_packet_feature": {"fl_dur":61,"src_ip": "192.
168.10.3","src_port":61745,"dst_ip": "192.168.10.1","dst_port"
:53,"tot_all_pkt":2,"tot_all_pkt_size":305,"tot_send_pkt":1,"tot_
send_pkt_size":199,"tot_recv_pkt":1,"tot_recv_pkt_size":106,"send_
pkt_max_size":199,"send_pkt_min_size":199,"send_pkt_avg_size":199,
"send_pkt_std_size":0,"recv_pkt_max_size":106,"recv_pkt_std_
size":0,"fl_byt_s":305,"fl_pkt_s":2,"fl_iat_avg":61,"fl_iat_s
td":0,"fl_iat_max":61,"fl_iat_min":61,"send_iat_tot":0,"send_
iat_avg":0,"send_iat_std":0,"send_iat_max":0,"send_iat_min":0,
"recv_iat_tot":0,"recv_iat_avg":0,"recv_iat_std":0,"recv_iat_
max":0,"recv_iat_min":0,"send_pkt_s":1,"recv_pkt_s":1,"pkt_l
en_min":106,"pkt_len_max":199,"pkt_len_avg":152.5,"pkt_len_st
d":46.5,"send_psh_flag":0,"recv_psh_flag":0,"send_urg_flag":0,
"recv_urg_flag":0,"fin_cnt":0,"syn_cnt":0,"rst_cnt":0,"psh_c
nt":0,"ack_cnt":0,"urg_cnt":0,"ece_cnt":0,"cwr_cnt":0,"send_
seg_avg":0,"send_seg_min":0,"recv_seg_avg":0,"send_win_byt":0,
"recv_win_byt":0,"send_act_pkt":0,"send_hdr_len":42,"recv_hdr_
len":42,"protocol": {"id": 1,"name": "TCP"}, "application": {"id": 632,
"name": "Google Shared Services"}, "tcp_session": "not-finished"
816973
```

특징 정보 학습된  
AI 모델

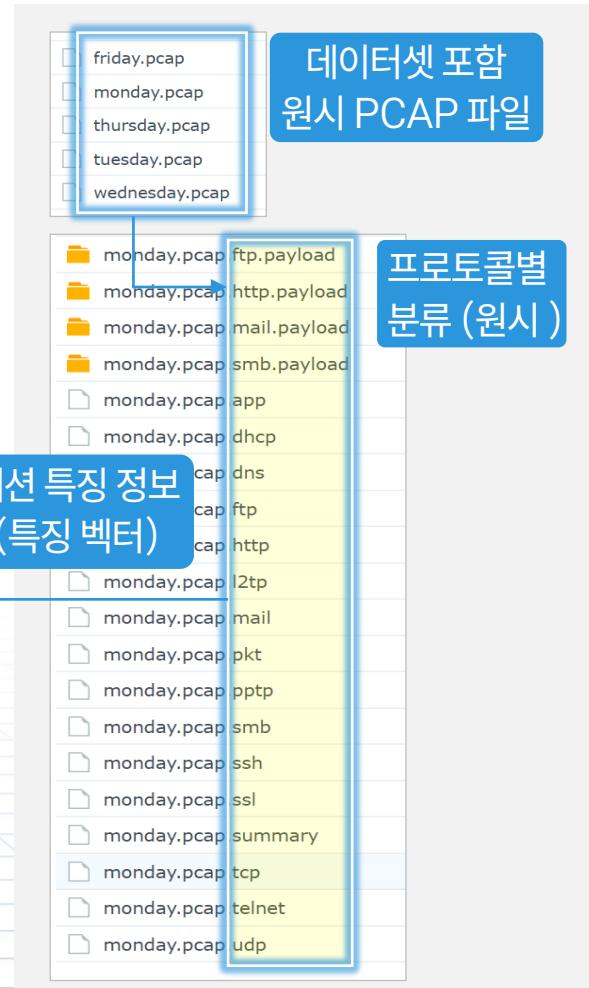


프로토콜과  
어플리케이션 식별



```
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
"recv_pkt_min_size": 60,
"recv_pkt_avg_size": 459.8,
"recv_pkt_std_size": 589.7,
"fl_byt_s": 9700,
"fl_pkt_s": 32,
"fl_iat_avg": 11.2,
"fl_iat_std": 15.4,
"fl_iat_max": 37,
"fl_iat_min": 0,
"send_iat_tot": 77,
"send_iat_avg": 11,
"send_iat_std": 16.5,
"send_iat_max": 37,
"send_iat_min": 0,
"recv_iat_tot": 160,
"recv_iat_avg": 20,
"recv_iat_std": 22.8,
"recv_iat_max": 64,
"recv_iat_min": 0,
"send_pkt_s": 15,
"recv_pkt_s": 17,
"pkt_len_min": 60,
"pkt_len_max": 1569,
"pkt_len_avg": 303.1,
"pkt_len_std": 467.1,
"send_psh_flag": 8,
"recv_psh_flag": 9,
"send_urg_flag": 0,
"recv_urg_flag": 0,
"fin_cnt": 0,
"syn_cnt": 2,
"rst_cnt": 0,
"psh_cnt": 17,
"ack_cnt": 31,
"urg_cnt": 0,
"ece_cnt": 0,
"cwr_cnt": 0,
"send_seg_avg": 89.2,
"send_seg_min": 20,
"recv_seg_avg": 424,
"send_win_byt": 32,
"recv_win_byt": 7335,
"send_act_pkt": 8,
"send_hdr_len": 858,
"recv_hdr_len": 960
"protocol": {
  "id": 30,
  "name": "SSL"
}
"application": {
  "id": 632,
  "name": "Google Shared Services"
}
```

라벨링 데이터 (어플리케이션)



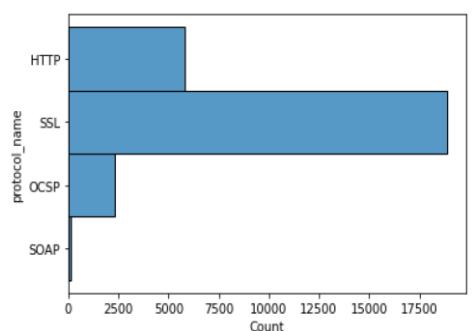
## 2. AI DPI 분석

### - AI DPI 모델 검증 결과

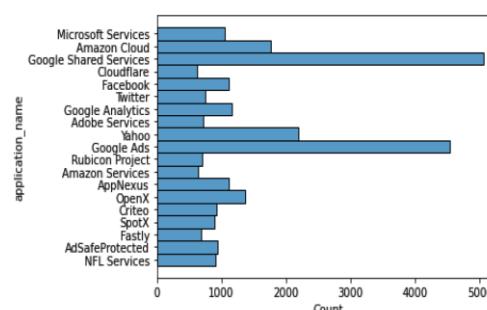
#### 원시 데이터 (pcap)으로 부터 특징 추출

target	src_ip	src_port	dst_ip	dst_port	l4_protocol	fl_dur	tot_all_pkt	tot_all_pkt_size	tot_send_pkt	...	send_seg_avg	send_seg_...
166	0	192.168.10.5	49176	134.170.115.55	443	6.0	139.0	5.0	495.0	3.0	...	87.0
199	0	192.168.10.14	49433	131.253.61.80	80	6.0	140.0	8.0	1293.0	5.0	...	82.8
222	0	192.168.10.14	49434	131.253.61.80	443	6.0	0.0	7.0	6149.0	3.0	...	83.7
228	0	192.168.10.14	49435	65.152.202.208	80	6.0	133.0	7.0	948.0	4.0	...	94.8
275	0	192.168.10.14	49441	23.50.75.27	80	6.0	47.0	7.0	2773.0	4.0	...	81.8
...	...	...	...	...	...	...	...	...	...	...	...	...
1054732	0	192.168.10.3	55166	23.211.102.137	80	6.0	76.0	15.0	3496.0	7.0	...	365.4
1055143	0	192.168.10.14	59152	64.4.54.254	443	6.0	549.0	19.0	9040.0	10.0	...	361.6
1055299	0	192.168.10.14	59153	23.21.84.138	443	6.0	152.0	13.0	4789.0	7.0	...	144.6
1055343	0	192.168.10.12	48284	23.63.226.81	80	6.0	77.0	7.0	1158.0	4.0	...	108.0
1055467	0	192.168.10.8	10399	184.84.243.218	80	6.0	249.0	7.0	1096.0	4.0	...	96.0

#### 프로토콜 분포



#### 어플리케이션 분포



#### AI 모델 검증 (프로토콜)

Model	Accuracy	AUC	Recall	Prec.	F1	Kappa	MCC	TT (Sec)
...	0.9922	0.9993	0.9558	0.9922	0.9922	0.9830	0.9831	1.0990
...	0.9856	0.9988	0.9558	0.9922	0.9922	0.9830	0.9831	0.1210
...	0.9514	0.9988	0.9558	0.9922	0.9922	0.9830	0.9831	0.8040
...	0.9431	0.9988	0.9558	0.9922	0.9922	0.9830	0.9831	0.9010
...	0.9267	0.9988	0.9558	0.9922	0.9922	0.9830	0.9831	0.1490
...	0.8310	0.8374	0.6035	0.8356	0.8244	0.6348	0.6436	0.5730
...	0.8309	0.0000	0.4878	0.8318	0.8080	0.5630	0.6027	0.0230
...	0.7029	0.5194	0.2906	0.6370	0.5198	0.8679	0.7102	0.7837

9종 AI 모델 검증

#### AI 모델 검증 (어플리케이션)

Model	Accuracy	AUC	Recall	Prec.	F1	Kappa	MCC	TT (Sec)
...	0.8814	0.9898	0.8816	0.8845	0.8806	0.8692	0.8697	1.3380
...	0.8251	0.9988	0.9558	0.9922	0.9922	0.9830	0.9831	0.1500
...	0.671	0.9988	0.9558	0.9922	0.9922	0.9830	0.9831	0.8040
...	0.512	0.9988	0.9558	0.9922	0.9922	0.9830	0.9831	0.9010
...	0.442	0.9988	0.9558	0.9922	0.9922	0.9830	0.9831	0.1490
...	0.3982	0.9988	0.9558	0.9922	0.9922	0.9830	0.9831	0.7260
...	0.3479	0.7958	0.3280	0.4015	0.3472	0.2877	0.2931	0.7780
...	0.2249	0.7526	0.2940	0.4058	0.2249	0.1700	0.1801	0.7400
...	0.1186	0.6166	0.1900	0.1600	0.1186	0.0600	0.0601	0.7070

9종 AI 모델 검증

[비공개]가 가장 좋은 결과 도출 (88%)  
→ 어플리케이션의 경우 좀 더 복잡한  
통신 구조를 가지고 있어 탐지율 낮음

## 2. AI DPI 분석

### - AI DPI 식별 결과

**Free Proxy List - List of Open Proxy Servers**

Proxy Server List - this page provides and maintains the largest and the most up-to-date list of working proxy servers that are available for public use. Our powerful software checks over a million proxy servers daily, with most proxies tested at least once every 15 minutes, thus creating one of the most reliable proxy lists on the Internet - all for free.

Any proxy server listed on this page can be used with a software application that supports the use of proxies such as your web browser. The most popular uses of proxies include hiding your real IP address, disguising your geographic location, and accessing blocked websites.

This proxy list is updated once every 60 seconds from the data stored in our gigabyte-sized proxy database. The list can be filtered down by a number of attributes such as the port number of a proxy, country of origin of a proxy, and the level of anonymity of a proxy. You can also view this list [on a map](#).

**Note:** If you do not know what any of these numbers mean, or how to use proxy servers in general, scroll to the bottom of this page.

< All Countries > < All Proxies >

Proxy IP	Proxy Port	Last Check	Proxy Speed	Uptime	Proxy Country	Anonymity
8.221.141.88	9080	16 mins ago	2695 ms	88% (24)	Japan - Tokyo	Elite
89.116.34.113	80	16 mins ago	2790 ms	34% (27)	India - Mumbai	Elite
80.194.38.106	3333	16 mins ago	5196 ms	9% (23)	United Kingdom - Hyde	Transparent

네트워크 및 인터넷 > 프록시

프록시 서버 편집

프록시 서버 사용: 켜기

80.194.38.106 3333

다음 항목으로 시작하는 주소를 제외하고 프록시 서버를 사용합니다. 여러 항목은 세미콜론(;)으로 구분합니다.  
127.0.0.1:16105;127.0.0.1:16106;localhost;  
127.0.0.1:21300

로컬(인트라넷) 주소에 프록시 서버 사용 안 함

저장 취소

2024-10-23 ~ 2024-10-30 CSV

날짜 선택: 2024-10-23 00:00:00 종료일: 2024-10-30 23:59:59

통계

# SRC IP	건수	# DST IP
1 10.10.5.122	4,390	1 142.250.196.238
2 10.10.0.11	2,094	2 142.250.71.142
3 10.10.0.12	1,931	3 142.250.199.78
4 10.10.0.105	1,478	4 142.250.222.14
5 10.10.0.87	1,241	5 142.250.197.42
6 10.10.0.92	752	6 142.250.76.238
7 10.10.5.65	726	7 118.126.201.5
8 10.10.5.40	712	8 142.250.196.238
9 10.10.5.38	692	9 142.250.199.206
10 10.10.5.175	672	10 142.250.71.238

시작일 ↓ 종료일 ↑ SRC IP SRC Port DST IP DST Port Protocol Application Count (Send / Recv) ↓ Bytes (Send / Recv) ↓

4 2024-10-30 20:50:17	2024-10-30 20:50:35	10.10.0.15	57584	80.194.38.106	3333	ssl	YouTube	65 (39 / 26)	37.6 KB (28.5 KB / 9.1 KB)
3 2024-10-30 20:45:38	2024-10-30 20:45:45	10.10.0.15	56534	80.194.38.106	3333	ssl	YouTube	75 (37 / 38)	52.3 KB (17.8 KB / 34.5 KB)
2 2024-10-30 20:44:27	2024-10-30 20:45:28	10.10.0.15	58983	80.194.38.106	3333	ssl	YouTube	211 (84 / 127)	176.0 KB (9.9 KB / 166.1 KB)
1 2024-10-30 20:44:32	2024-10-30 20:45:28	10.10.0.15	59009	80.194.38.106	3333	ssl	YouTube	390 (145 / 245)	349.1 KB (12.7 KB / 336.5 KB)

443 ssl YouTube 50 (23 / 27) 18.1 KB (4.1 KB / 13.9 KB)

443 ssl YouTube 2,110 (621 / 1,489) 2.1 MB (441 KB / 2.1 MB)

443 ssl YouTube 43 (20 / 23) 16.9 KB (5.2 KB / 11.7 KB)

443 quic YouTube 31 (14 / 17) 16.8 KB (3.1 KB / 7.7 KB)

443 quic YouTube 19,348 (2,308 / 17,058) 21.1 MB (271.5 KB / 20.8 MB)

443 ssl YouTube 67 (41 / 46) 50.3 KB (4.8 KB / 45.5 KB)

프록시로 포트 변경해도, 트래픽 특징으로 식별하기 때문에 어플리케이션 (YouTube) 정확하게 식별 가능

## 2. AI DPI 분석

### - AI DPI TTA 검증 결과

G4B(www.g4b.go.kr) 진위 확인 코드 : ootvx+PzOGE=

시험성적서

한국정보통신기술협회  
소프트웨어시험인증연구소  
주소: 경기도 성남시 분당구 분당로 47  
전화: 031-780-9137, Fax: 031-724-0189

성적서번호: BT-A-21-0498

TTA

1. 의뢰자  
· 회사(기관)명 : 남산조립  
· 주 소 : (06143) 서울특별시 강남구 선릉로 577 조선내화빌딩 4층, 산조립  
· 계약일자 : 2021.12.27.

2. 시험성적서의 용도 : 과제 산출물 검증용

3. 제품명 : AI 기반 사이버 위협 탐지 및 유형 분류 도구

4. 버전 : v1.0

5. 시험장소 : □ 고정시험실, ■ 현장시험  
· 시험수행주소 : (주)산조립, 서울특별시 강남구 선릉로 577 조선내화빌딩 4층

6. 시험기간 : 2021. 12. 28. ~ 2022. 1. 4.

7. 시험방법 :  
- 상세 내용은 “<3. 시험항목 및 방법>” 참고

8. 시험환경 : 실온, 실습

9. 시험결과 : BT-A-21-0498-GR 참조

비고 : 1. 이 성적서의 시험결과는 의뢰자에 의해 제공된 시험품에 한하여 용도 이외의 사용을 금합니다.  
2. 이 성적서는 KS Q ISO/IEC 17025 및 KOLAS 인정 분야와 관련 없습니다.  
3. 이 성적서의 진위여부는 기업지원플러스(www.ptb.go.kr)에서 진위확인코드로 확인 가능합니다.

확인인	작성자 성명 : 조경우	승인자 직책 : 기술책임자 성명 : 신준호
-----	-----------------	-------------------------------

2022년 1월 4일

한국정보통신기술협회 회장

TPS-0071-3(01)

G4B(www.g4b.go.kr) 진위 확인 코드 : ootvx+PzOGE=

5. 시험결과

시험 항목별 시험 결과는 아래와 같다. (상세 시험 결과는 “<6. 시험기록>” 참고)

ID	시험항목	시험목표 및 기준	결과	비고
TC1	침해사고 예-탐지 메이터셋 메타데이터 생성 정확도	<p>&lt;시험목표&gt; 수집된 http 프로토콜 원천데이터에 대한 메타데이터 생성 정확도 확인</p> <p>&lt;시험기준&gt;</p> <ul style="list-style-type: none"> <li>기준: 원천데이터에 포함된 http request 주소와 시험의뢰기업이 사전에 생성한 메타데이터의 http request 주소의 일치 여부 확인</li> <li>산정식: <math>X = \frac{A}{B}</math> <ul style="list-style-type: none"> <li>- A: 원천데이터와 메타데이터의 http request 주소 일치 수량</li> <li>- B: 원천데이터 총 수량</li> </ul> </li> </ul>	X = 1	-
TC2	침해사고 예-탐지 기반 프로토콜 및 어플리케이션 식별 정확도	<p>&lt;시험목표&gt; TC1의 메타데이터와 레이블을 기반으로 학습한 시험대상 제품(모델)의 프로토콜 및 어플리케이션 식별 정확도 확인</p> <p>&lt;시험기준&gt;</p> <ul style="list-style-type: none"> <li>기준: 프로토콜 및 어플리케이션 식별모델별 다중 분류 성능</li> <li>산정식: Accuracy(%) = <math>\frac{\text{결과 일치 샘플수}}{\text{전체 샘플수}} \times 100</math></li> </ul>	프로토콜 식별모델 98.10%	-
TC3	침해사고 예-탐지 메이터셋 기반 공격, 정상 이벤트 구분 정확도	<p>&lt;시험목표&gt; TC1의 메타데이터와 레이블을 기반으로 학습한 시험대상 제품(모델)의 이벤트 분류 정확도 확인</p> <p>&lt;시험기준&gt;</p> <ul style="list-style-type: none"> <li>기준: 이벤트(공격/정상) 이진 분류 성능</li> <li>산정식: Accuracy(%) = <math>\frac{\text{결과 일치 샘플수}}{\text{전체 샘플수}} \times 100</math></li> </ul>	93.40%	-

TPS-0071-4(00) Copyright 2021 TTA 페이지 (24/30)

TC5

\* System event log: 원천데이터-12,199건 / 학습데이터-12,199건

No.	속성명	유형	전처리 후 특성 수
1	action	범주형	10
2	event_id	범주형	10
3	event_time	텍스트(연속형)	5
4	host	범주형	3
5	level	범주형	5
6	logtype	범주형	4
7	payload	텍스트(연속형)	10
8	source	범주형	10
		계	57

\* 성능 결값은 시험 로그, 코드 및 모델링 결과 파일(.csv)을 통해 확인함

TC6

- 시험대상 제품(모델)의 분류 성능은 평균 99.90%로 확인됨

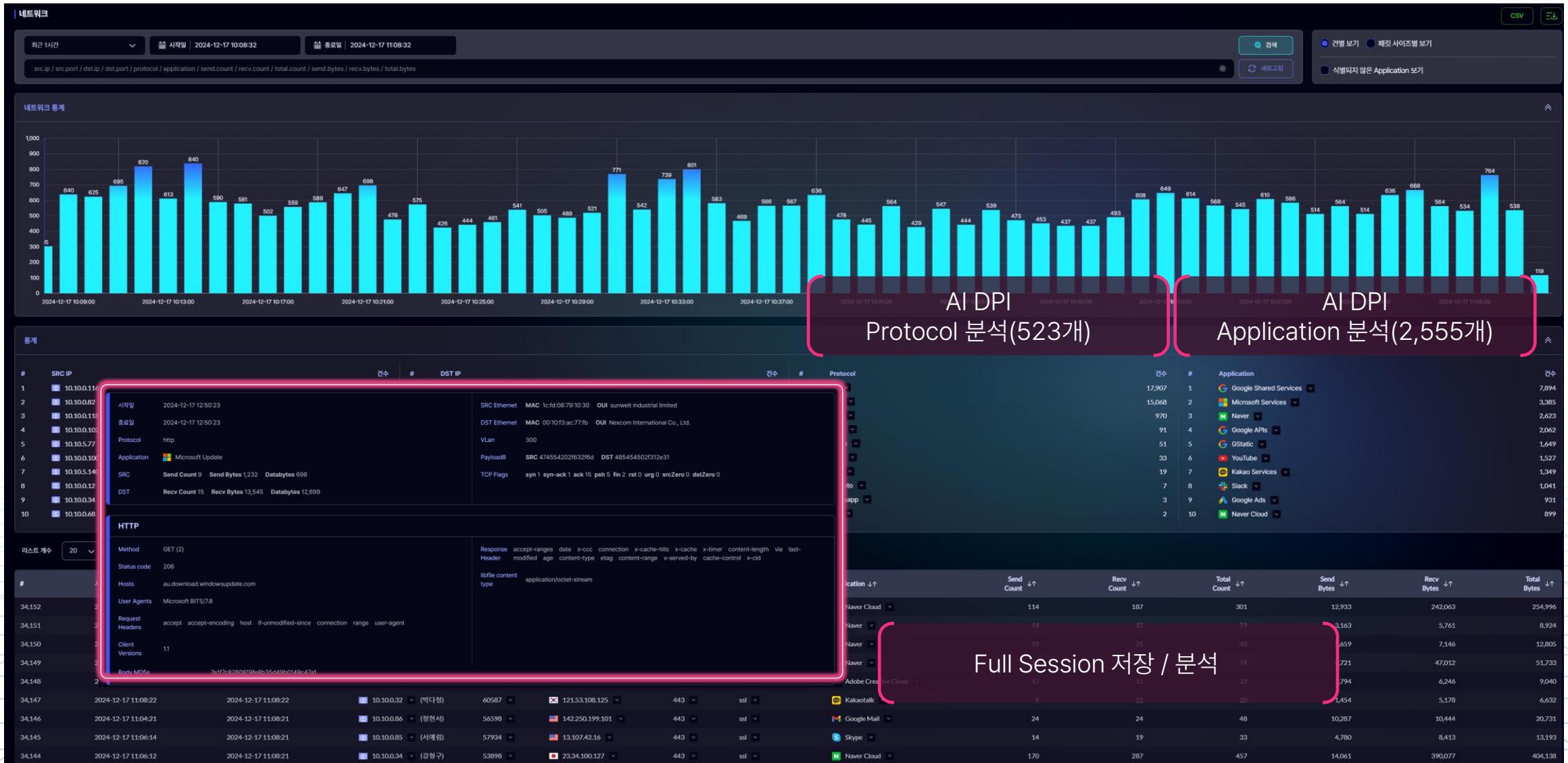
장비 유형	측정 결과		
	Precision	Recall	F1-Score
FW (Firewall)	RF 99.92%	XG 99.98%	99.95%
IPS (Intrusion Detection System)	RF 99.95%	XG 99.98%	99.97%
IDS (Intrusion Detection System)	RF 98.87%	100%	99.43%
WAF (Web Application Firewall)	RF 99.43%	XG 100%	99.72%
WEB Access log	RF 100%	XG 100%	100%
System event log	RF 100%	XG 100%	100%
	평균 (F1-Score)		99.90%

\* RF: Random Forest, XG: XGBoost

\* 성능 결값은 시험대상 제품의 로그 및 모델링 결과 파일(.csv)을 통해 확인함

## 2. AI DPI 분석

### - WEB



## 2. AI DPI 분석 - WEB

■ SRC IP : Port 102.1.51.61:42968 ■ DST IP : Port 104.17.39.19:443

PCAP X

시작일	2024-11-25 10:14:20	SRC Ethernet	MAC 00:00:5e:00:01:64 00:06:c4:90:1d:73	OUI ICANN, IANA Department Prolink Inc.
종료일	2024-11-25 10:17:20	DST Ethernet	MAC cc:82:7f:14:0a:16	OUI Advantech Technology (CHINA) Co., Ltd.
Protocol	-	Payload8	SRC 474554202f646174 DST 485454502f312e31	
Application	A -	Tags	pcap-disk-overload	
SRC	Send Count 13 Send Bytes 1,810 Databytes 1,034	TCP Flags	syn 1 syn-ack 1 ack 127 psh 10 fin 2 rst 0 urg 0 srcZero 0 dstZero 0	
DST	Recv Count 128 Recv Bytes 174,710 Databytes 167,778			

### HTTP

Method	GET (1)	Response	cache-control	last-modified	age	date	report-to	etag	content-length	nel	expires	cf-cache-status
Status code	200	Header	server	vary	content-type	accept-ranges	server-timing	cf-ray	connection	alt-svc		
Hosts	av19a.com	server	Header	cloudflare								
User Agents	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 Edg/131.0.0.0	libfile content	image/jpeg									
Request Headers	host sec-ch-ua-full-version-list sec-ch-ua-full-version sec-fetch-dest sec-fetch-site sec-ch-ua-form-factors sec-ch-ua-mobile accept-encoding sec-ch-ua-wow64 sec-fetch-mode accept-language accept sec-ch-ua-platform-version sec-ch-ua-bitness user-agent connection sec-ch-ua-model referer sec-ch-ua-arch sec-ch-ua-platform sec-ch-ua	type										
Client Versions	1.1											

24-11-25 10:17:20 102.1.51.61 42967 104.17.39.19 443 A 8 27 35 150

## 2. AI DPI 분석

### - WEB

시작일	2025-01-17 13:08:07	SRC Ethernet	MAC 00:00:0c:07:ac:64 5c:83:8f:30:54:7f	OUI Cisco Systems, Inc
종료일	2025-01-17 13:08:08	DST Ethernet	MAC b4:0c:25:ef:c0:49 c4:00:ad:ab:2a:9d	OUI Palo Alto Networks Advantech Technology (CHINA) Co., Ltd.
Protocol	ssl	Payload8	SRC 1603010200010001 DST 485454502f312e30	
Application	A -	Tags	acked-unseen-segment-dst	
SRC	Send Count 8 Send Bytes 1,052 Databytes 524	TCP Flags	syn 1 syn-ack 1 ack 3 psh 2 fin 3 rst 3 urg 0 srcZero 0 dstZero 2	
DST	Recv Count 5 Recv Bytes 1,702 Databytes 1,388			

#### HTTP

Status code	200	Response Headers	pragma connection content-type
Hosts	newtoki467.com	libfile content-type	text/html

#### TLS

JA3	1aad9aff2523e91bbf4e8276a5b2140e	JA4	t13d2114h2_abf72aed6336_14788d8d241b
-----	----------------------------------	-----	--------------------------------------

## 2. AI DPI 분석 - WEB

1 2025-01-06 16:40:56 2025-01-06 16:40:56 10.50.2.89 58234 185.88.181.6 443 ssl A Xvideos - PCAP

시작일	2025-01-06 16:40:55	SRC Ethernet	MAC 04:62:73:ad:01:bf	00:00:0c:07:ac:64	OUI Cisco Systems, Inc						
종료일	2025-01-06 16:40:56	DST Ethernet	MAC b4:0c:25:ef:c0:49	c4:00:ad:ab:2a:9d	OUI Palo Alto Networks Advantech Technology (CHINA) Co, Ltd.						
Protocol	ssl	Payload8	SRC 1603010200010001	DST 485454502f312e30							
Application	A Xvideos	Tags	acked-unseen-segment-dst	acked-unseen-segment-src	out-of-order-dst						
SRC	Send Count 8 Send Bytes 1,045 Databytes 517	TCP Flags	syn 1	syn-ack 1	ack 14	psh 2	fin 2	rst 7	urg 0	srcZero 0	dstZero 1
DST	Recv Count 19 Recv Bytes 7,660 Databytes 1,392										

### HTTP

Status code	200	Response Headers	pragma	connection	content-type
Hosts	xvideos.com	libfile	content-type	text/html	
Body MD5s	b815f7cabcb2799dd40e7fc6a7fa76ef				

### 3. 탐지 - WEB



AI 분석 결과, **2025-04-18 21:36:23 ~ 2025-04-25 21:36:23** 기간 동안 **총 538개**의 네트워크 위협이 탐지되었습니다. 이는 전체 **10,471,057개**의 세션 중 **174,608개**의 세션에서 발생했으며, 전체 트래픽의 **1.67%**에 해당하는 **위협 수준**으로 분석됩니다. 탐지된 위협과 관련된 **내부 IP는 18개**, **외부 IP는 39개**로 확인되었습니다.

발생 시간: 최근 7일 | 2025-04-18 21:36:23 ~ 2025-04-25 21:36:23

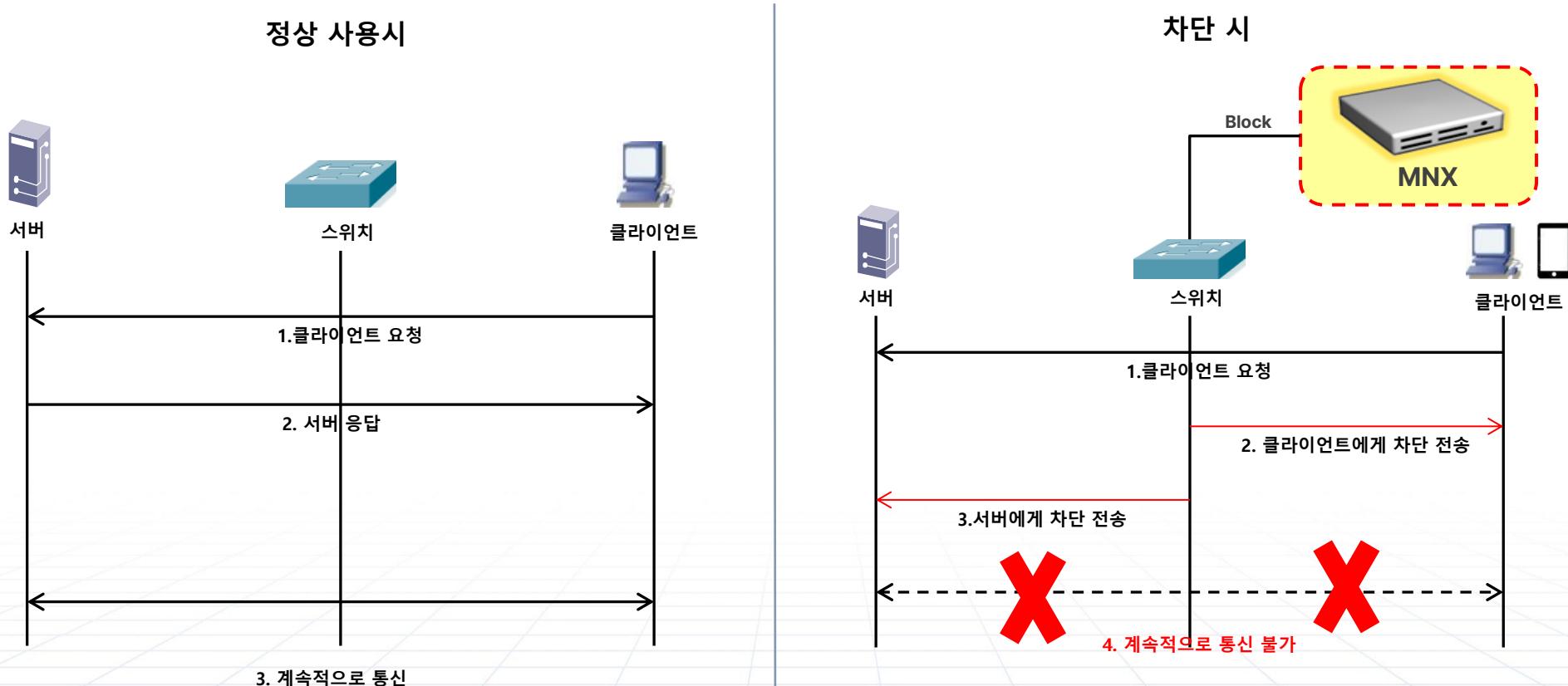
위협도: 전체 | 검색 필드 선택

진행 중으로 변경 | 완료로 변경

#	Ticket-ID	발생 시간	플레이북 명	기준 조건	위협도	SRC IP
458	1623	2025-04-25 18:16:25	유해사이트 접속탐지(성인사이트)	출발지 IP	하	10.10.0.60
457	1622	2025-04-25 18:06:25	유해사이트 접속탐지(성인사이트)	출발지 IP	하	10.10.0.60
456	1621	2025-04-25 17:56:25	유해사이트 접속탐지(도박사이트)	출발지 IP	하	10.10.0.60
455	1620	2025-04-25 17:46:25	유해사이트 접속탐지(성인사이트)	출발지 IP	하	10.10.0.60
454	1619	2025-04-25 17:36:25	유해사이트 접속탐지(불법웹툰사이트)	출발지 IP	하	10.10.0.60
453	1618	2025-04-25 17:26:25	[AI 위협 탐지] 내부 단일 호스트에서 다...	출발지 IP	상	10.10.0.60
452	1617	2025-04-25 17:16:25	[AI 위협 탐지] 내부 단일 호스트에서 다...	출발지 IP	상	10.10.0.60

## 4. 대응

### - TCP 세션 차단

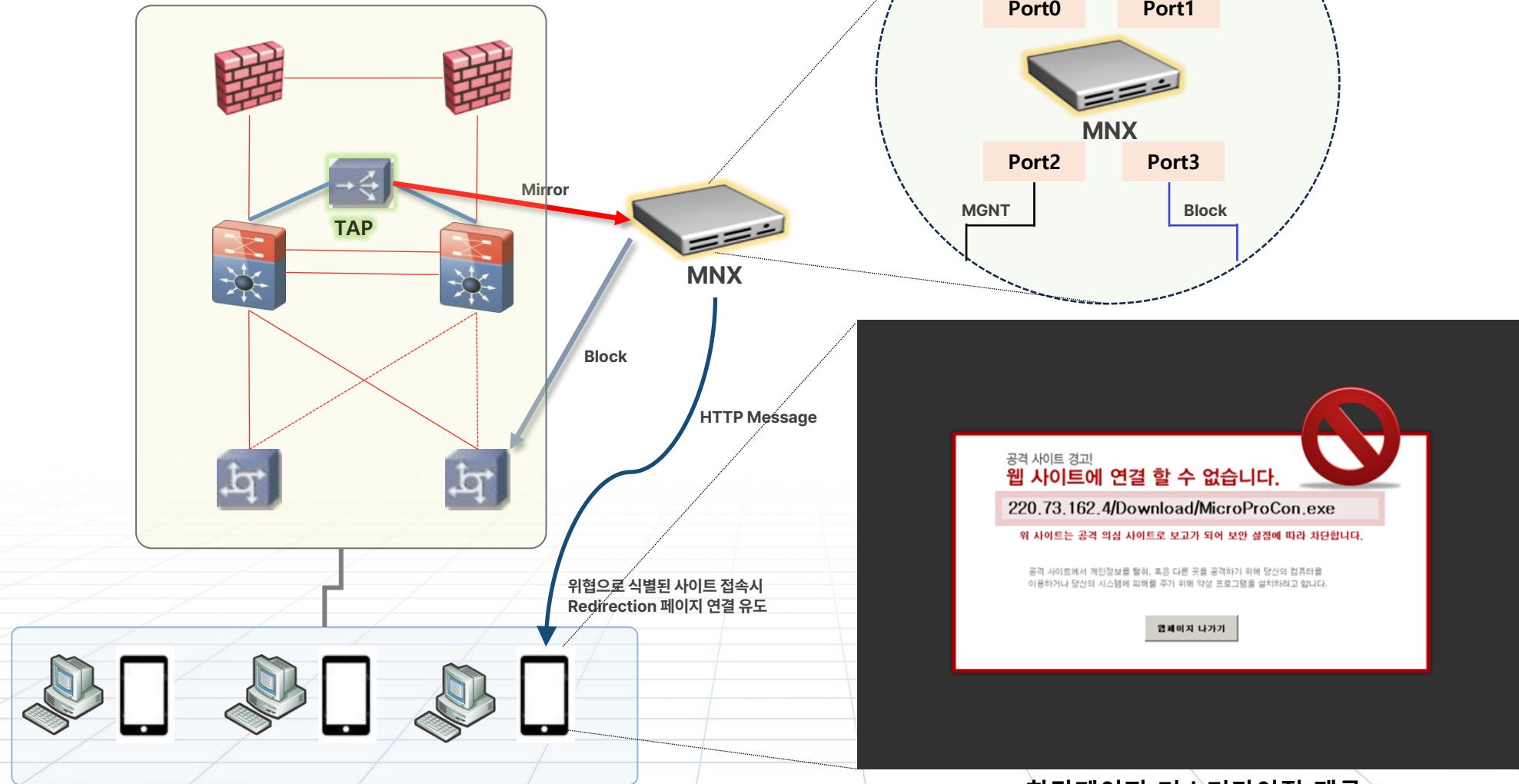


RST 기반 차단.

- RST 패킷이 클라이언트(단말기)로 도달할수 있어야하며, 네트워크 장비에 의해 드롭되지 않아야 합니다.

## 4. 대응

### - HTTP Redirection

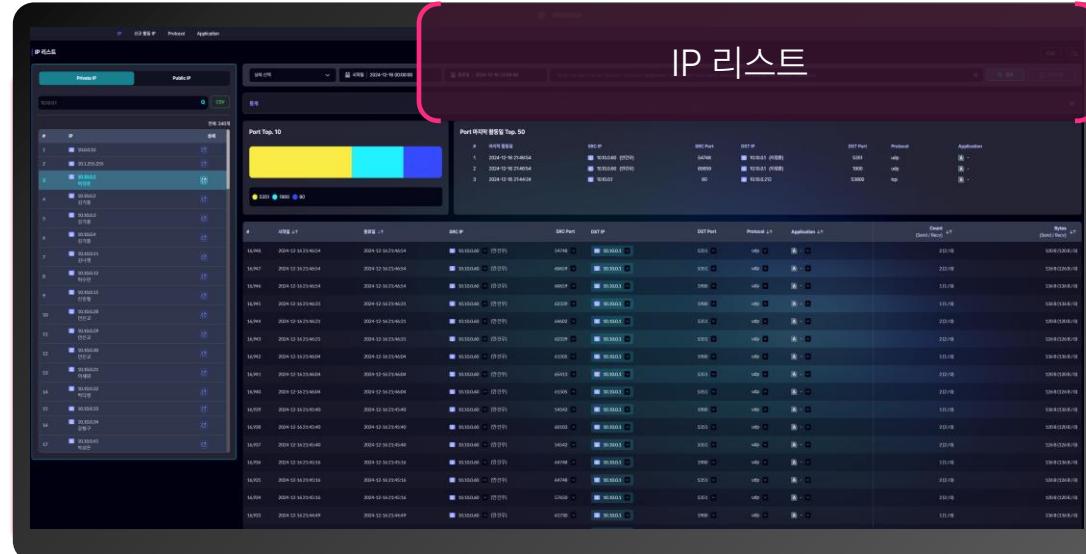


차단시 Redirection 페이지 제공

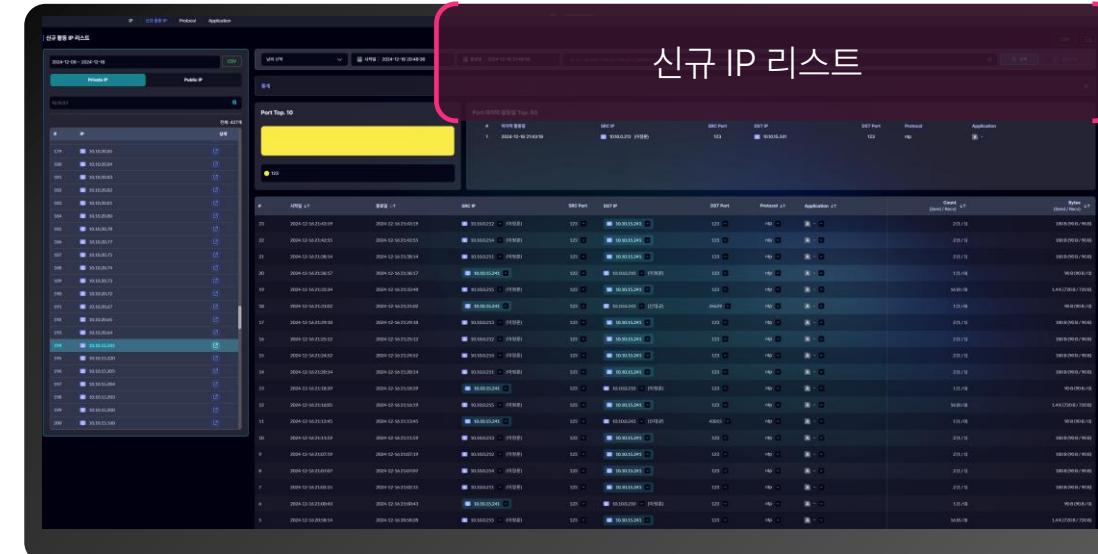
- 복호화장비를 통해 암호화 트래픽에 대해 복호화 트래픽을 받아야만 가능합니다.

차단페이지 커스터마이징 제공

## 5. 가시화 - 트래픽 활동



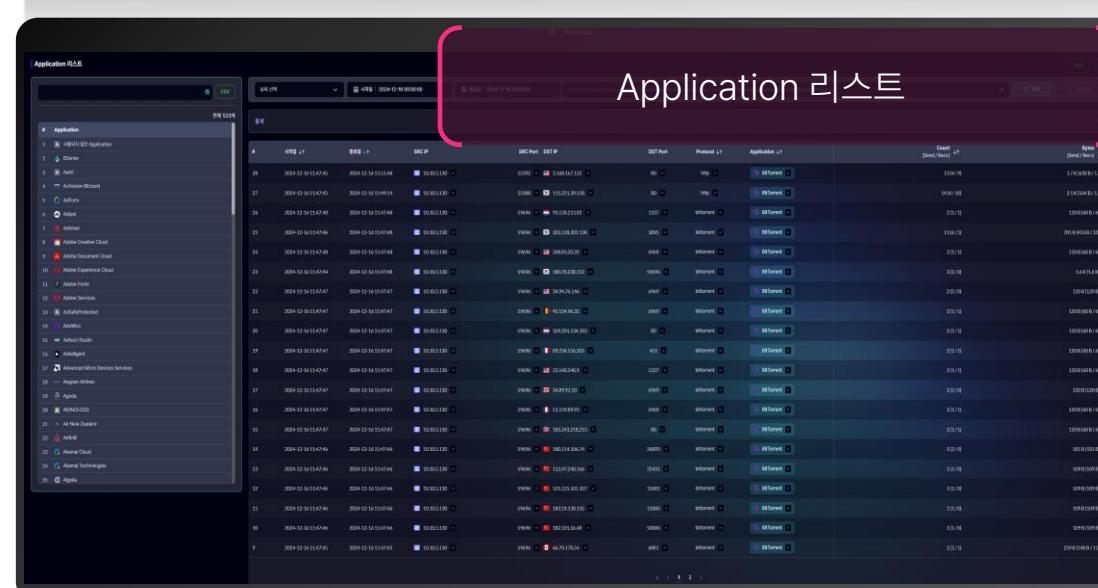
## IP 리스트



## 신규 IP 리스트



## Protocol 리스트



## Application 리스트

**Security,  
AI,  
Network,  
Data for  
Society**

**SANDS Lab** 

경기도 과천시 과천대로7나길 25, 12F  
02-704-7502  
[www.sandslab.io](http://www.sandslab.io)