# 위협 정보공유를 통한 대응의 필요성

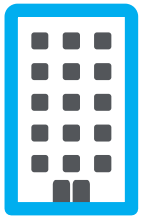
**Trellix Korea**

**Sr. Enterprise Account Manager 윤성욱 상무**

Trellix

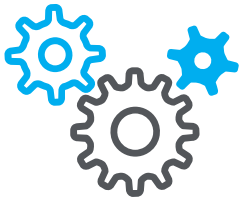
# 위협의 영향

고도화된 표적
공격으로 인해
기업이 계속해서
피해를 입음



기업은 끊임없이
위협대응을 위해
보안에 투자하고 있음

고립된 제품운영은
단편적인 가시성 및
제어 부족



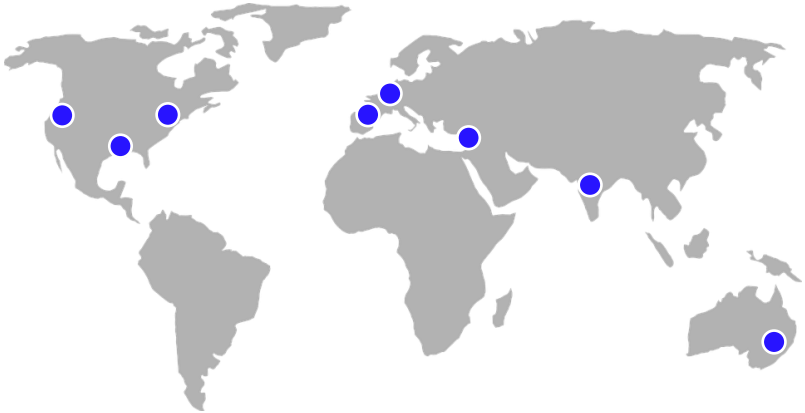
위협에 대한
느리고 리소스
집약적인 대응

# Trellix Threat Intelligence 를 통해 리스크 및 위협 운영 조정

| Threat Readiness Problems | Causes | Solution |
| --- | --- | --- |
| “당신은 위협에 놓여 있습니까? 우선 순위는 무엇입니까? ” | 글로벌 가시성, 우선 순위 | 글로벌 위협 정보와 동향 |
| “여러분은 민감한가요 ? 보호가 유지될 수 있나요?” | 영향 예측, 우선 순위 지정 | 보안 위험 평가 |
| “보호를 유지하려면 무엇을 바꿔야 합니까?” | 사전 예방적 적응 | 대책을 능동적으로 조정 |

# Trellix Global Threat Intelligence

## 글로벌 인텔리전스 및 로컬 가시성으로 강력한 방어 Platform 구축



**+50**
TI Analysts

**+200**
researchers

- 멀티 시간대에 위치하여 연중 무휴 24시간 서비스 제공
- 원격 및 현장에서 분석가 지원
- 러시아어, 중국어, 베트남어, 프랑스어, 독일어, 스페인어, 포르투갈어, 히브리어, 아랍어, 네덜란드어를 구사하는 원어민 분석가
- 분석가로부터 취약점및 악성코드 연구까지 다양한 기술 제공
- 국가 CERTS, IC 기관, LE 기관, 국방 및 상업조직에 이르는 다양한 고객 층 보유
- 인텔리전스부터 제품까지 데이터 기반 연구
- 전 세계적으로 10억 개 이상의 센서를 통한 SIGINT 정보



Trellix

# South Korea - Threat Landscape (1 Week)

Total – Detections: 6,724,585

Campaign – Detections: 4,650

Detections correlated to threat actor activity

Total - Unique MD5s: 170

Number of files after duplicates are removed and each file can be detected more than once. The separate detections combined equal the total detections.

Campaign - Unique MD5s: 170

Number of files that are correlated to known threat actor activity

Total - Unique Customers: 10

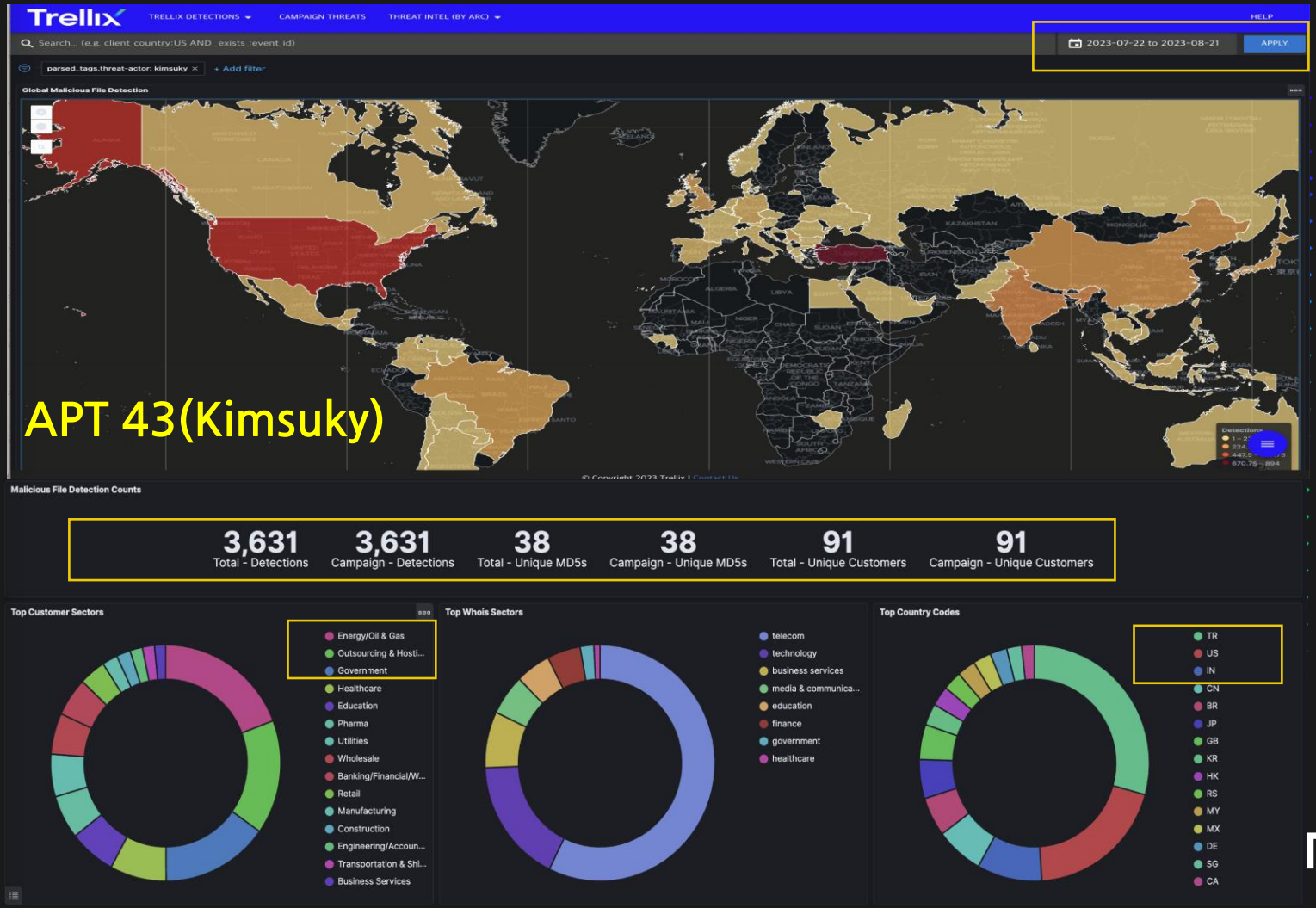
Number of customers after duplicates are removed

Campaign - Unique Customers: 10

Number of organizations that the Campaign – Unique MD5s are correlated to




Trellix


Trellix
TRELLIX DETECTIONS
CAMPAIGN THREATS
THREAT INTEL (BY ARC)
HELP
Search... (e.g. client_country:US AND _exists_:event_id)
2023-07-22 to 2023-08-21
APPLY
parsed_tags.threat-actor: kimsuky
+ Add filter
Global Malicious File Detection
APT 43(Kimsuky)
Malicious File Detection Counts
3,631
Total - Detections
3,631
Campaign - Detections
38
Total - Unique MD5s
38
Campaign - Unique MD5s
91
Total - Unique Customers
91
Campaign - Unique Customers
Top Customer Sectors
Energy/Oil & Gas
Outsourcing & Hosti...
Government
Healthcare
Education
Pharma
Utilities
Wholesale
Banking/Financial/W...
Retail
Manufacturing
Construction
Engineering/Accoun...
Transportation & Shi...
Business Services
Top Whois Sectors
telecom
technology
business services
media & communica...
education
finance
government
healthcare
Top Country Codes
TR
US
IN
CN
BR
JP
GB
KR
HK
RS
MY
MX
DE
SG
CA



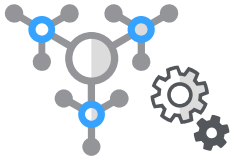
Trellix

# 위협정보 교환의 필요성

## 협업 위협 인텔리전스 에코시스템 구축

내부 및 외부
평판 집계

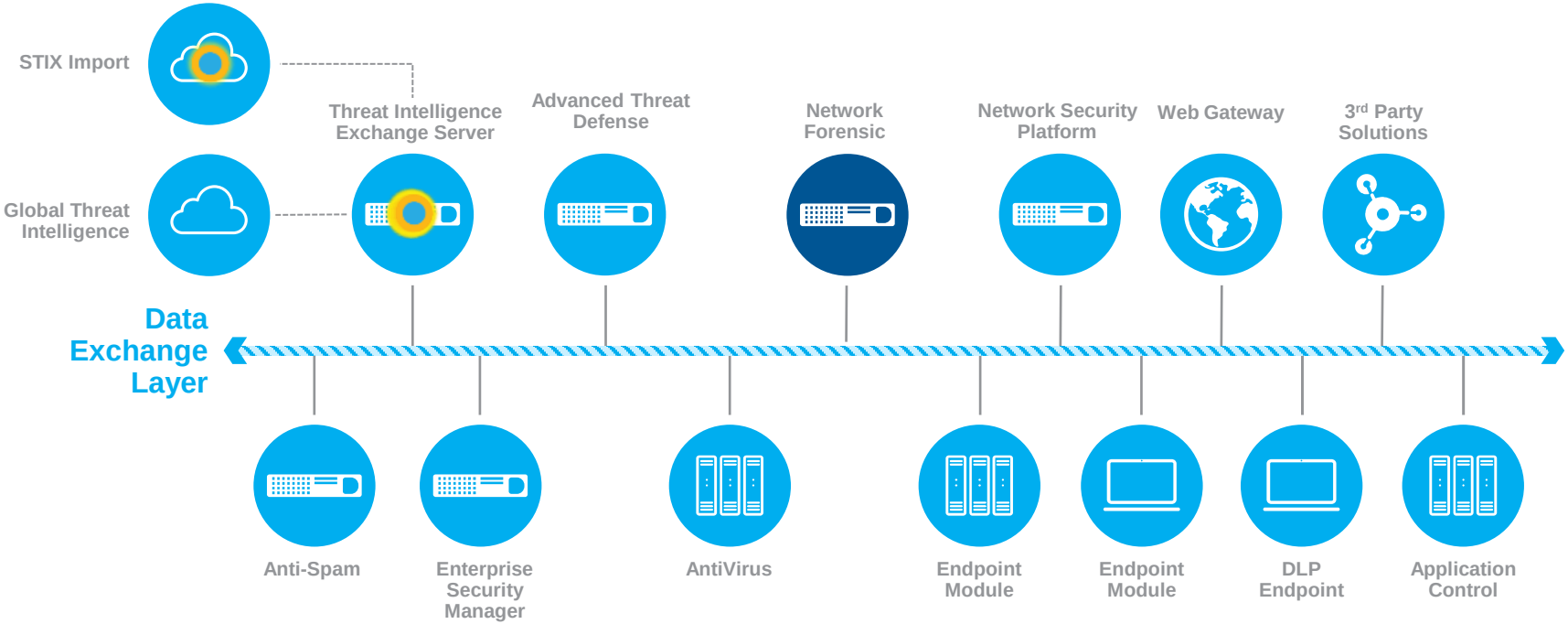
전체 에코시스템에서
평판 인텔리전스를
즉시 공유



알 수 없는 파일에
대한 심층 분석
자동화

로컬 제어 및
가시성 확보

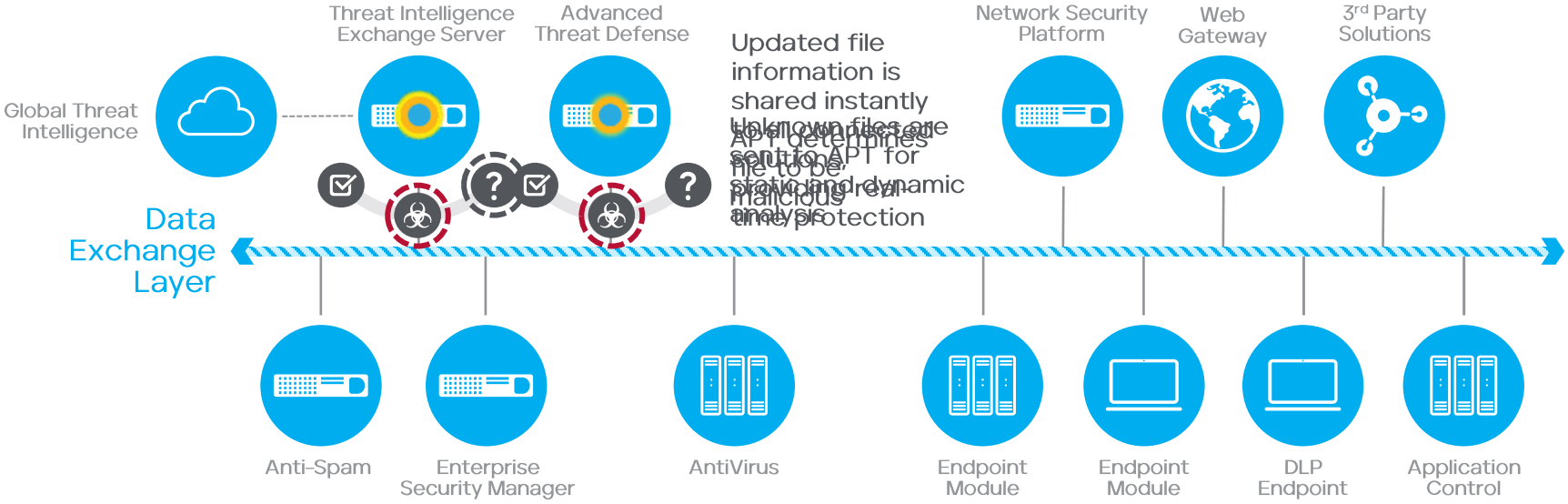
# 위협정보 교환 모델






Trellix

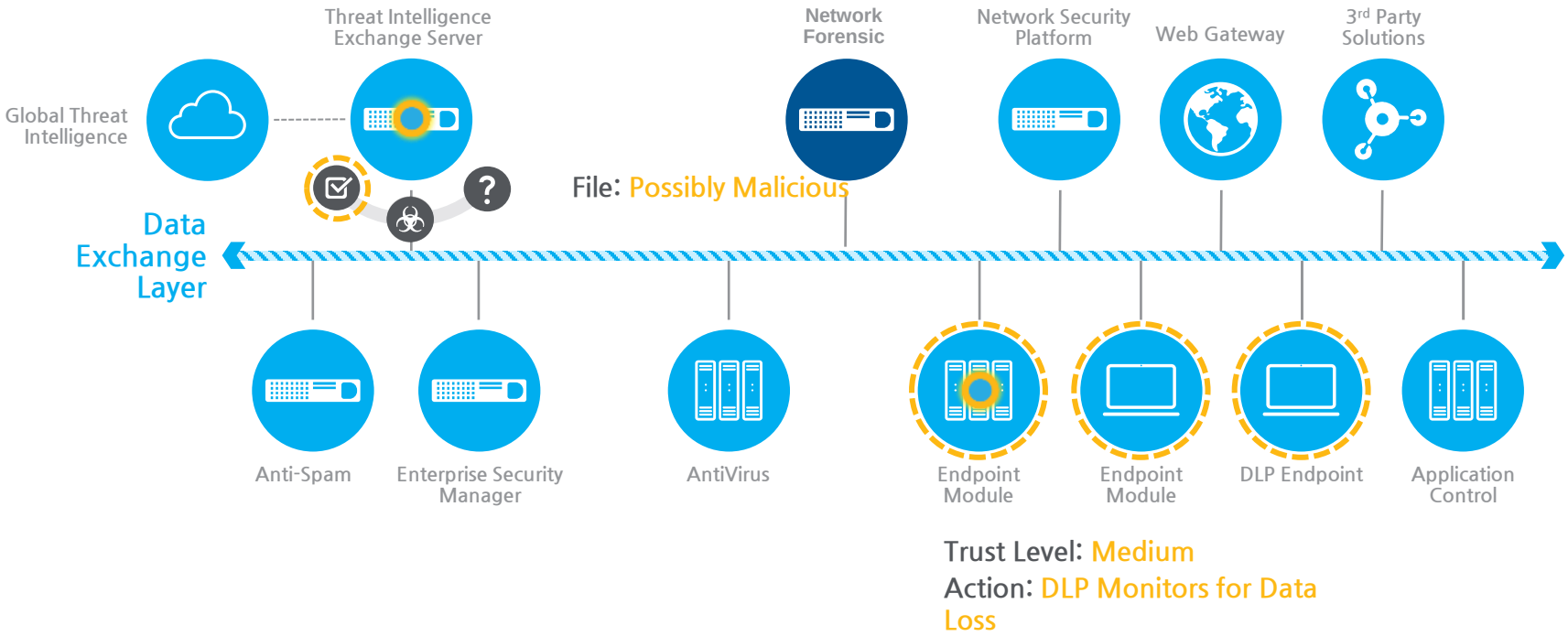
# APT와 연계한 정보의 교환






Trellix

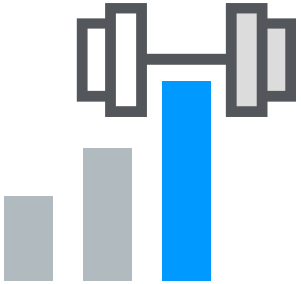
# End-Point와 연계한 정보 공유



# 마지막으로

보안 제품이 함께
작동해야 합니다

보안 제품은 서로
배워야 합니다.



보안 제품은 시간이
지남에 따라 더욱
강화되어야 합니다.

# Trellix 로 더 빠르고 정확하게 대응하세요.

Trellix