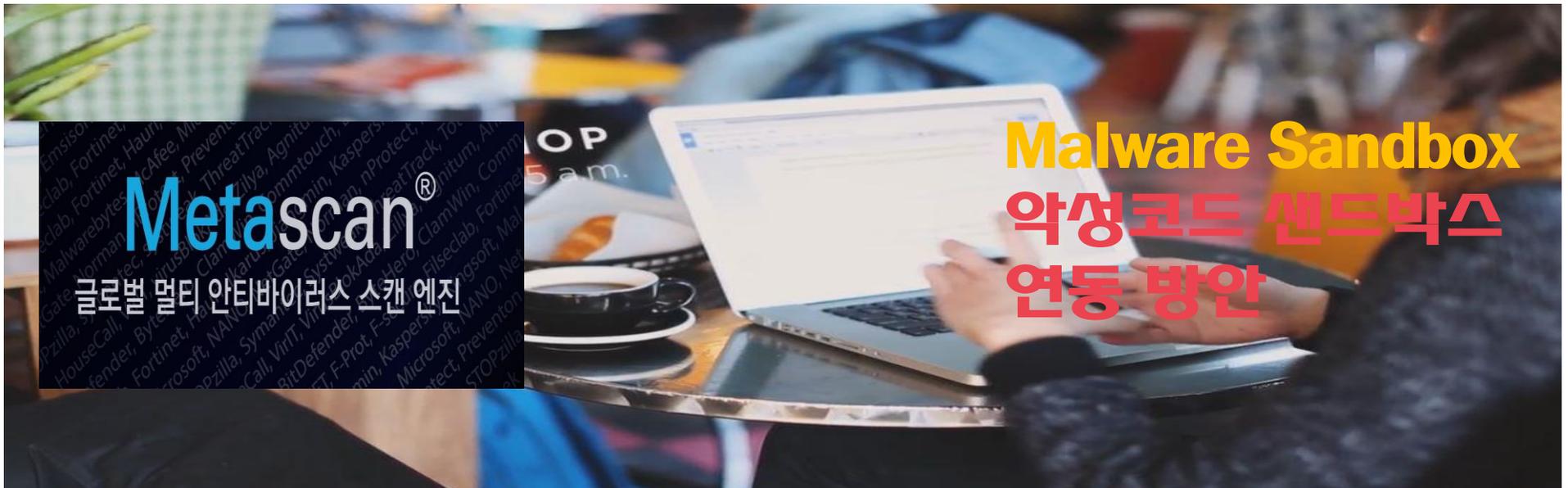


Metascan[®]

APT 공격, 신종 및 변종 악성코드 탐지 솔루션



Metascan[®]
글로벌 멀티 안티바이러스 스캔 엔진

Malware Sandbox
악성코드 샌드박스
연동 방안

악성코드 탐지 어떻게 할 것인가?



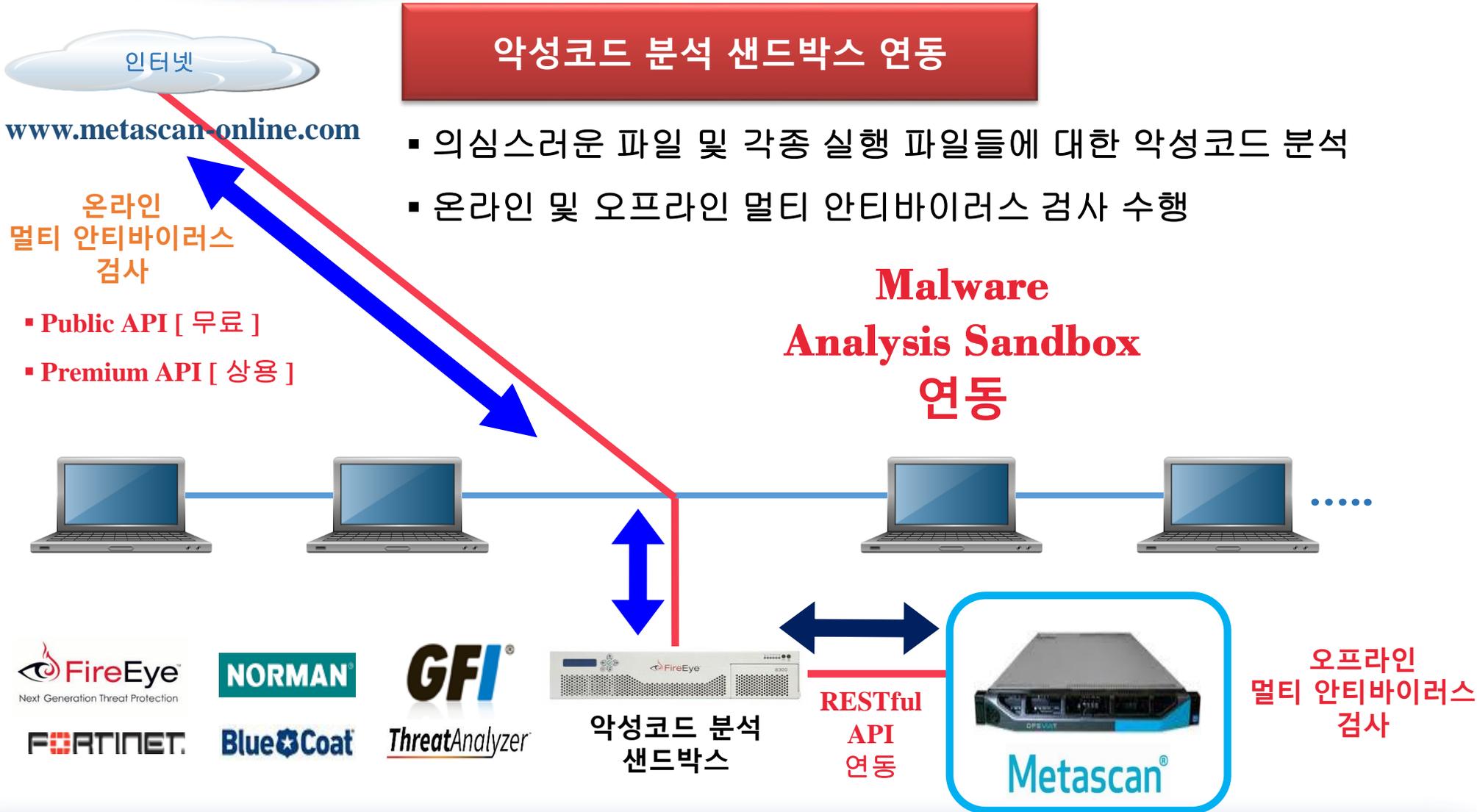
탐지해야만
차단할 수 있습니다!

[구성 사례]

Malware Sandbox 악성코드 샌드박스 연동 방안



Metascan 구성안 [악성코드 분석 샌드박스 연동]



Metascan 멀티 안티바이러스 스캔 엔진

악성코드 분석
샌드박스

동적분석

탐지율

정확성

멀티 안티바이러스 스캔
엔진

향상!

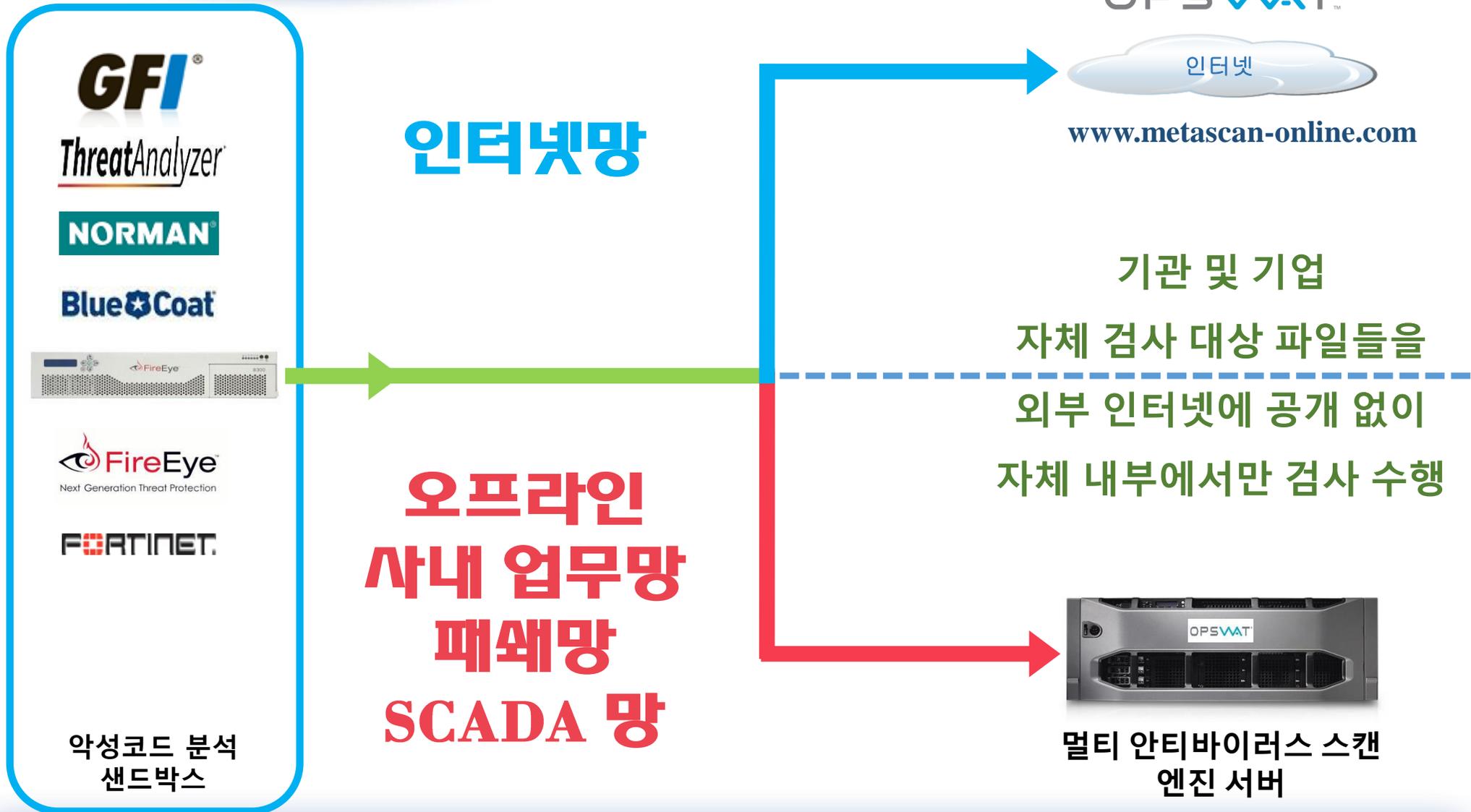
패턴분석

글로벌 30개 안티바이러스 스캔

- Ahnlab, Avira
- ESET, ClamWin
- Bitdefender, Total Defense
- ThreatTrack, Qiuck Heal
- nProtect, AVG
- Kaspersky, F-PROT
- Emsisoft, VirusBlokAda
- K7 Computing Agnitum
- MacAfee, Filseclab, STOPzilla
- Symantec, IKARUS
- F-Secure, HouseCall™, AntiSpyware
- MicroSoft, NANO antivirus,
- Trend Micro, Zillya, LAVASOFT,

휴리스틱 분석

Metascan 멀티 안티바이러스 스캔 엔진

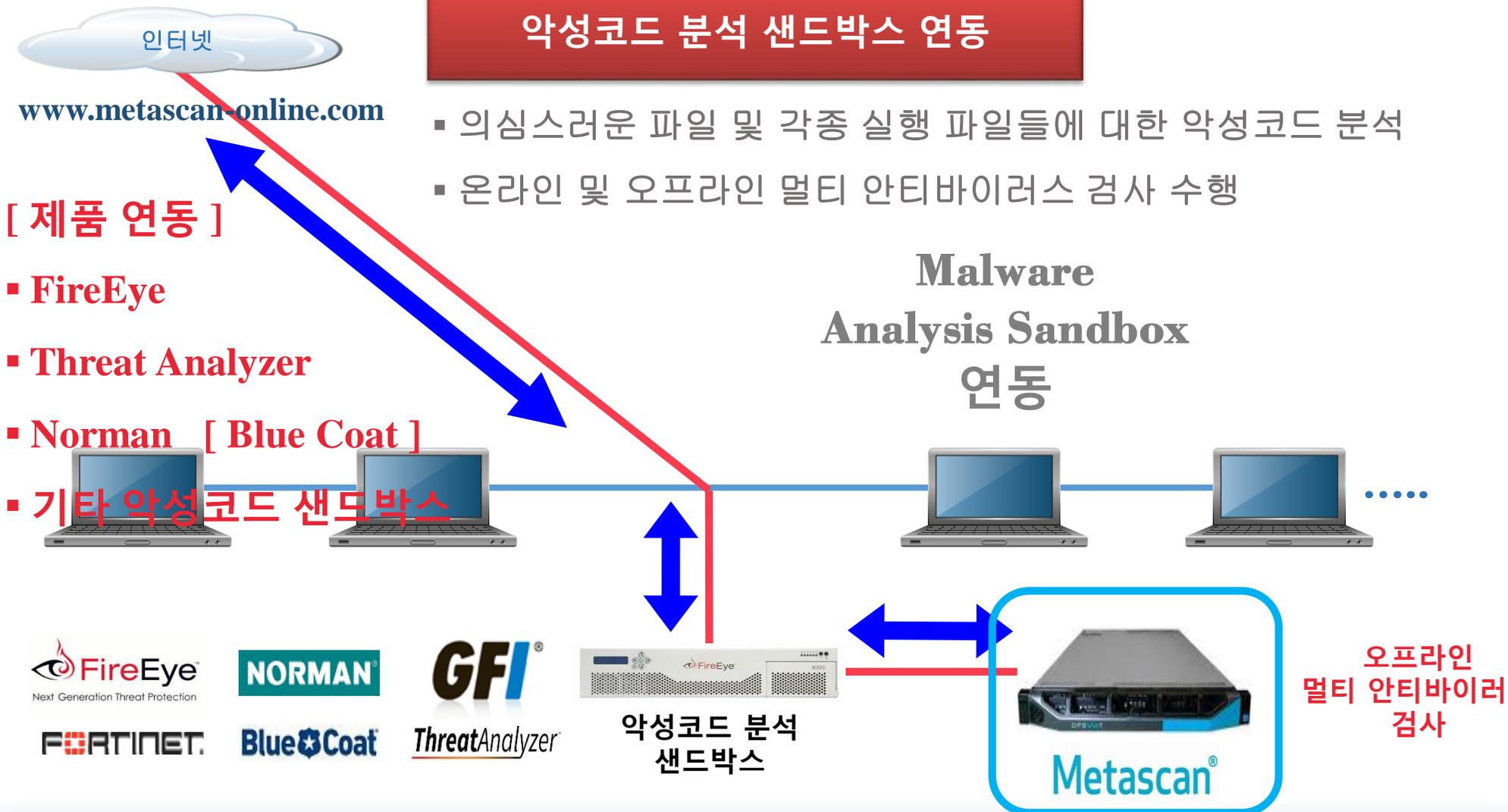


Metascan 구성안 [악성코드 분석 샌드박스 연동]

악성코드 분석 샌드박스 연동

- 의심스러운 파일 및 각종 실행 파일들에 대한 악성코드 분석
- 온라인 및 오프라인 멀티 안티바이러스 검사 수행

Malware Analysis Sandbox 연동



[제품 연동]

- FireEye
- Threat Analyzer
- Norman [Blue Coat]
- 기타 악성코드 샌드박스

