Fortinet AI ATP Solution

# 포티넷 인공지능 ATP 솔루션

## 가상 보안 분석가

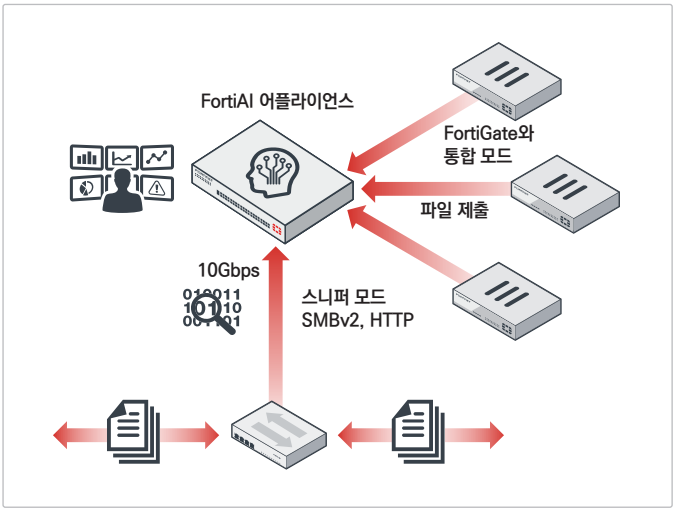
숙련 된 보안 분석가를 모방하기 위하여 인공지능 DNN(Deep Neural Networks)을 사용, 위협을 분류하여 보안 관제(SecOps)를 강화합니다.

## 위협 원천 차단

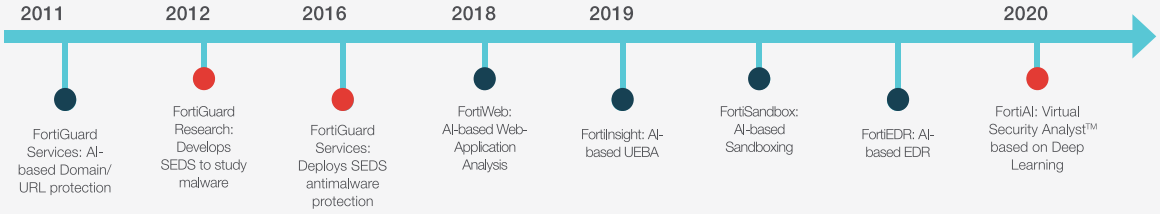
지속적으로 진화하는 학습 알고리즘을 기반으로 위협 특성을 과학적으로 분석하여 1초 이내에 정확한 판정을 생성함으로써 조직이 위협에 노출되는 시간을 크게 줄입니다.

## 진화하는 인공지능

FortiAI의 온 프레미스 AI 학습은 조직의 특정 트래픽을 분석하고 즉각적으로 직면하는 새로운 위협에 적응함으로써 오탐을 줄입니다.




### Fortinet의 AI 및 ML 개발 역사




## FortiAI 모델별 기능 역할

| | FortiAI-3500F | FortiAI-VM16 | FortiAI-VM32 |
|---|---|---|---|
| 처리량(시간당) | 100,000 | 14,000 | 22,000 |
| 초 단위 탐지 | ○ | ○ | ○ |
| 스니퍼 처리량 | 10 Gt | Hypervisor Hardware Dependent | Hypervisor Hardware Dependent |
| GPU 가속 기능 | ○ | × | × |
| 엔진 코어 | · 인공지능인 DNN을 이용한 악성코드 분석<br>· 시나리오 기반 엔진을 이용하여 최초 악성코드 근원지 탐지<br>· 유사성 엔진을 이용하여 네트워크에서 변종 악성 코드를 탐지<br>· MITRE ATT&CK 악성코드 매핑 | · Pre-trained 되어 있는 수백만 개의 악성코드 DB<br>· 아웃브레이크(Outbreak) 검색 엔진 (hash, virus family)<br>· 파일 침해 지표 IOC (Indicator of Compromise) 분석 | |
| 디플로이먼트 | · 스탠드 얼론 : 스니퍼 모드<br>· FortiGate와 연동 가능<br>· ICAP 커넥터 지원 | | |
| REST API 지원 | ○ | ○ | ○ |
| Hypervisor Support | N/A | ESXi 6.7 U2+ and KVM | ESXi 6.7 U2+ and KVM |
| 인터페이스 | 2 x 10 GE RJ45 (10/100/1000), 1 x GE RJ45 IPMI, 1 x RJ45 Console | Hypervisor Hardware Dependent | Hypervisor Hardware Dependent |

| 파일 유형 및 프로토콜 |
|---|
| 32bit / 64bit PE 파일<br>– PE 파일<br>– DLLs<br>– 실행 ZIP 파일 |
| 웹 / 텍스트 트래픽<br>– HTML, EXE, PDF, JS, VBS, VBA, DOC, PPT, XSLT, ELF, HWP (Hancom) |
| 스니퍼<br>– HTTP, SMBv2, IMAP, POP, SMTP |
| FortiGate 연동<br>– HTTP, HTTPS (SSL 복호화), SMTP, POP3, IMAP, MAPI, FTP |
| 수동 / REST API 업로드<br>– .tar, .gz, .tar.gz, .zip, .bz2, .rar |