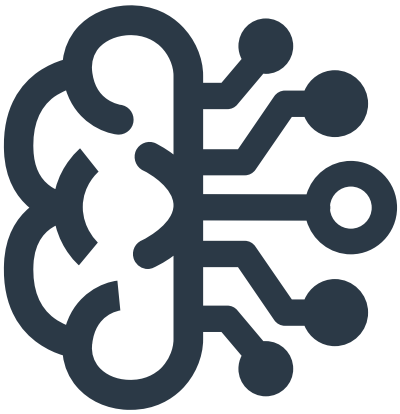
DATA SHEET

FortiAI

FortiAI-3500F

1초 이내에 판단하는
Virtual Security Analyst™

FortiAI는 보안 관제(SecOps) 팀을 위해 설계된 최신 AI 기반 보안 침해 보호 기술로, 정체를 교묘하게 숨긴 멀웨어 등을 포함한 멀웨어를 식별, 분류, 분석하도록 도와주는 훈련된 Virtual Security Analyst™를 통해 지능형 지속 위협을 방어합니다. FortiAI는 Advanced AI(Artificial Intelligence) 및 ANN(Artificial Neural Network)의 특허 출원* 중인 기술로 딥 러닝 기술을 활용하여 즉시 위협을 방지하고 다양한 종류의 합성된 위협 및 감염을 복구 업데이트하기 위한 오케스트레이션된 대응을 설계하도록 도와줍니다. FortiAI는 몇 년간 심혈을 기울인 FortiGuard Labs 연구에 기초하여 "탐지에 걸리는 시간"을 크게 단축해 기업과 고객을 보호해줍니다.



*특허 출원 #U.S.16/053,479

현재 직면한 최대의 SOC 문제

AI가 지원하는 사이버 공격

감염력이 큰 AI 위협이 SOC 내에 존재하는 모든 사소한 위협 취약성까지 알아내도록 설계된 자동 공격으로 사이버 시장을 와해시키고 있습니다.

데이터의 거대한 흐름

점점 더 복잡해지는 데이터 아키텍처들이 다양한 환경에서 여러 가지 공격 시나리오를 알아내기 위해 보안 관제에 무게를 싣고 있습니다.

정체를 감춘 멀웨어

교묘하게 설계된 보안 위협은 멀웨어 동작 방식을 숨겨 엔터프라이즈 시스템에 침투하고 SOC를 속입니다.

사이버 보안 경험의 부족

사이버 보안, 특히 침해 분석과 멀웨어 연구에서의 경험은 가장 획득하기 어렵습니다.

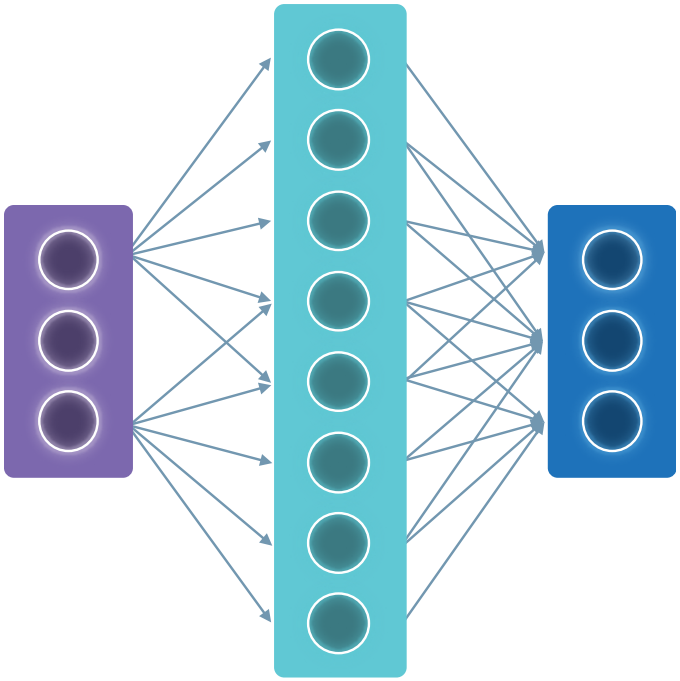
주요 특징

- 딥 러닝 AI 모델로 구동되는 Virtual Security Analyst™는 경험이 풍부한 보안 분석 전문가를 모방하여 위협 및 표면 멀웨어 감염을 조사하고 기기업의 보안 관제(SecOps)를 강화해줍니다.
- 지능이 뛰어난 AI는 600만 개 이상의 멀웨어 특성을 적용해 1초 이내에 판정을 내리며, 배포 첫날부터 새 기능을 학습합니다.
- 온프레미스 학습을 통해 기업의 특정한 트래픽을 분석하고 새롭게 위장한 위협에 적응해 오탐지를 줄여줍니다.
- 멀웨어 탐지 시간을 몇 분 단위에서 1초 이내로 낮춰줍니다.
- FortiAI의 딥 러닝, 즉 ANN을 사용하는 딥 신경망은 끊임없이 진화하는 학습 알고리즘을 기반으로 파일 기반 위협과 파일을 사용하지 않는 위협을 과학적으로 분석하고, 정체를 숨긴 위협까지도 노출합니다.

하이라이트

최첨단 인공 신경망(ANN)

- 최첨단 ANN은 FortiGuard Labs에서 2,000만 개 이상의 깨끗한 파일과 악성 파일로 사전 훈련을 하고 온프레미스에서 추가적인 훈련을 실행합니다. FortiGuard 네트워크에서는 ANN 모델을 업데이트하여 최신 위협으로부터 고객을 보호합니다. 멀웨어 유형을 20개 이상의 공격 시나리오로 분류하고, AI 기반 엔진으로 공격의 출처를 추적하며, 인간의 뇌가 작동하는 방식을 모방합니다.
- 멀티 태스크 위협 학습 프레임워크를 포함한 AI 기반 침해 보호 프로그램이 복잡한 보안 요구 사항을 하나의 고성능 네트워크 보안 어플라이언스로 통합합니다.
- 다계층 탐지 전략은 머신 러닝과 신경망 기술을 사용하여 AI가 지원하는 첨단 사이버 공격으로 인해 침해 후 손상이 발생하기 전에 딥 머신 러닝 기능을 제공합니다.
- 수백만 개의 알려진 깨끗한 샘플과 악성 샘플로 FortiGuard Labs에서 사전 훈련되어, 수십억 개의 정상적인 기능과 악성 기능의 차이를 습득합니다. 이는 기업의 보안 환경에 따라 악성 및 공격 유형을 과학적으로 판단하는 데 사용됩니다.



Virtual Security Analyst™

FortiAI 엔진의 역할:

- **공격 분류**(예시): 랜섬웨어, 웜 활동. 데이터 누출, 익스플로잇, 뱅킹 트로잔, 정교한 위협, 시나리오 발견적 위협, 크립토재킹, 백도어, 봇넷, Dos, 애플리케이션, 웹 쉘, 검색 엔진 오염, 제네릭 트로잔, 루트키트
- **공격 출처 조사 –** 타임스탬프를 포함하여 감염의 출처 추적
- **개인 멀웨어 분석 전문가** – 신경망 기반으로 멀웨어 유형을 과학적으로 판정하고 학습 경험에 따라 FortiAI 엔진을 자체적으로 구동

99.9%
탐지율*

<100 ms
1초 이내 탐지

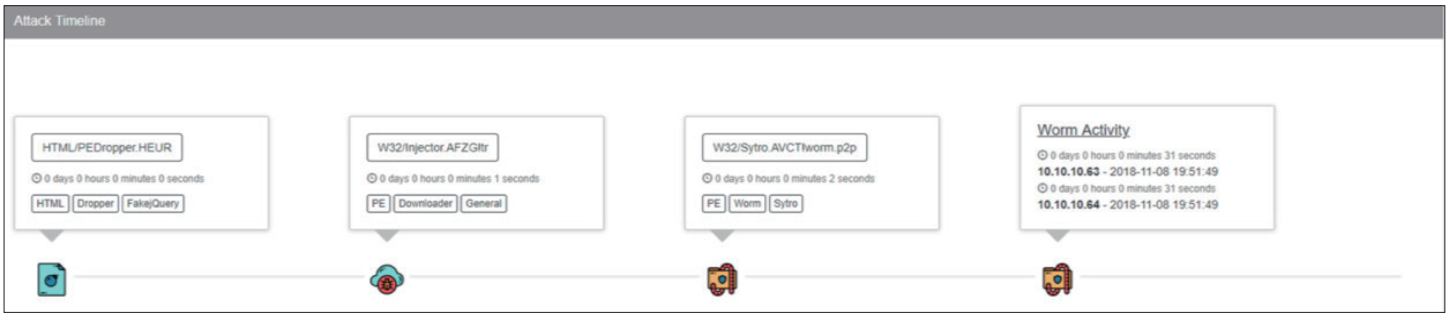
10G
네트워크 처리량

2,000억
노출된 기능

20+
공격 시나리오

*Breaking Point 멀웨어 공격 팩으로 측정

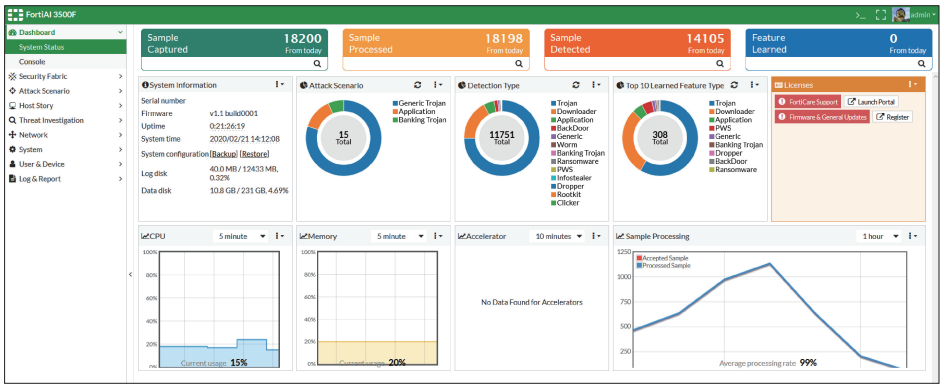
Virtual Security AnalystTM 웜 공격의 출처 추적



제품 기능

FortiAI-3500F

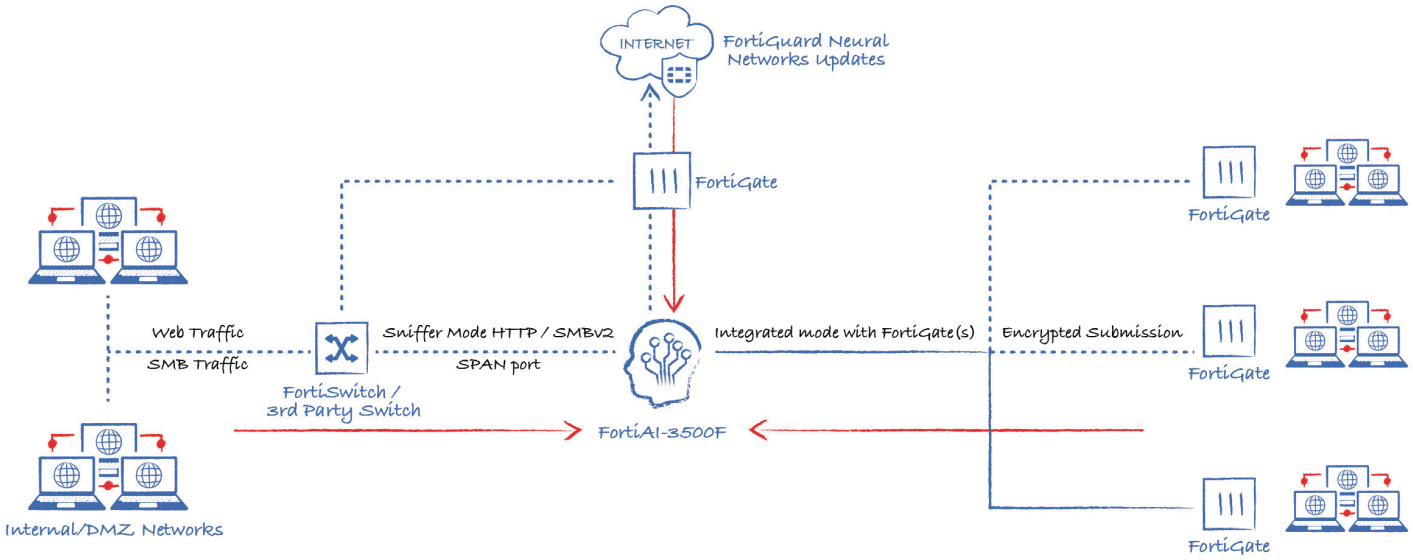
- 파일 유형 지원: 32bit 및 64bit의 실행 가능한 파일, 모든 PE(Portable Executables) 파일에 적용. HTML, VBA, VBS, JS, PDF, BAT, SH, PHP, XML, 파워 쉘 스크립트, MS Office 문서, PDF 등의 텍스트 기반 파일도 지원됩니다.
- ANN을 사용한 고급 멀웨어 분석 (인공 신경망)
- 제로 데이 멀웨어를 찾아내기 위해 사전 훈련된 기능(10억 단위)
- 공격 시나리오, 호스트 스토리 모드, 위협 조사 뷰



FortiAI-3500F 대시보드

- 로그 및 보고서 - 멀웨어의 MD5/SHA 해시, 소스/대상/타임스탬프/URL 분석.
- 추가적인 센서 불필요, 독립적 배포
- 운영 모드 포함: 독립적(sniffer) 및/또는 FortiGates와 통합
- 지원되는 프로토콜: 독립적/Sniffer 모드 프로토콜 지원: HTTP, SMBv2, FortiGate와의 통합 모드 HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM 및 이와 동등한 기술
- 네트워킹: 고정 라우트 지원, IPv4 지원, 시스템: 역할 기반 관리 지원(RBAC)

배포



사양

	FORTIAI-3500F
하드웨어 사양	
폼팩터	2RU 랙마운트
총 인터페이스	2 x 10GE RJ45(10/100/1000), 1 x GE RJ45 IPMI, 1 x RJ45 Console
스토리지 용량	2 x 3.84TB SSD, 총 7.68TB
기본 RAID 수준(소프트웨어 RAID)	1
이동형 하드 드라이브	✔
예비 핫스왑 전원	✔
시스템 성능	
처리량	시간당 100,000개 파일
1초 이내 판정	✔
Sniffer 처리량	Line Rate 10G
규격	
높이 x 너비 x 길이(in)	3.41 x 18.98(손잡이 포함) x 29.58(베젤 포함), 3.41 x 17.09(손잡이 포함) x 29.04(베젤 포함)
높이 x 너비 x 길이(mm)	86.8 x 482(손잡이 포함) x 751.34(베젤 포함), 86.8 x 434(손잡이 포함) x 737.5(베젤 포함)
중량	68.34lbs(31kg)
환경	
AC 전원	100-240VAC, 60-50Hz
전력 소비(평균/최대)	1,390W/1,668W
방열	6,824BTU/h
작동 온도	10~35°C(50~95°F), 장비에 직사광선이 닿지 않게 보관
보관 온도	–40~65°C(–40~149°F)
습도	보관: 5~95% RH, 이슬점 최대 33°C(91°F). 대기는 항상 비응결 상태여야 합니다. 작동: 10~80% 상대 습도, 29°C(84.2°F)
작동 고도	최대 7,400ft(2,250m)
규정 준수	
보안 인증	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB

*70/30 Non-PE/PE 파일에 기반한 실제 처리량 결합

주문 정보

제품	SKU	설명
FortiAI 3500F	FAI-3500F	제로 데이/멀웨어 탐지를 위한 FortiAI-3500F 어플라이언스. 인공 신경망(ANN) 기술 기반. 2 x 10Gb GE 코퍼 케이블(트랜시버 없이 10/1000/10000 지원)
FortiAI-3500F 하드웨어 번들	FAI-3500F-BDL-228-DD	FortiAI-3500F 번들 - 하드웨어 + 상시 FortiCare 및 FortiGuard Neural Networks 엔진 업데이트 및 기준치
FortiCare 및 업데이트	FC-10-AI3K5-228-02-DD	상시 FortiCare + FortiGuard 신경망 엔진 업데이트 및 기준치

www.fortinet.com/kr

서울특별시 강남구 영동대로 325에스타워 14 /15층 전화: 080-559-8989 Email: **kr-callcenter@fortinet.com**