DATA SHEET

FortiAI

Available in:

Appliance

Virtual Machine

Sub-second Investigation with Virtual Security Analyst™

FortiAI represents the future of AI-driven breach protection technology, designed for short-staffed Security Operation Center (SOC) teams to defend against various threats including advanced persistent threats through a trained **Virtual Security Analyst™** that helps you identify, classify, and respond to malware including those well camouflaged. FortiAI employs patent-pending* **Deep Neural Networks based on Advanced AI and Artificial Neural Network** to provide sub-second investigation by harnessing deep learning technologies to assist you in an automated response to remediate different breeds of synthesized AI and non-AI-based threats. Based on several years of FortiGuard Labs research, FortiAI reduces the "time to detect and respond" significantly to protect your organization.

*Patent pending #U.S.16/053,479

Shortage of Experienced SOC Analysts

Experience is the hardest thing to acquire in cyber security, especially in threat analysis, outbreak investigation, and malware research experience

Breach Prevention

Assist SecOps with AI-driven capabilities to handle high volumne or traffic, identify malware and anomalies hidden in network

Masqueraded Malware

Carefully crafted cyber threats designed to bypass your existing security controls through the camouflage of malware behaviors

AI-Powered Cyber Attacks

Innovative threat actors disrupt cybersecurity through automated attacks designed to overwhelm or sneak past your SOC defenses

Key Features

- **Virtual Security Analyst™** powered by a Deep Neural Networks AI model that augments your organizations' Security Operations (SecOps) by mimicking an experienced Security Analyst to investigate threats and surface malware outbreaks
- Reduces malware detection and investigation time from minutes to **Sub-second** verdict
- Mature AI that applies **6+ million malware features** to achieve sub-second verdicts for day-one deployment with the capability to learn new features
- **On-premise Learning** to reduce false positives by analyzing an organization's specific traffic and adapting to newly disguised threats
- Scientifically analyze zero days including fileless threats and classifies them into **20+ malware attack scenarios**
- Integrate into Fortinet's Security Fabric by uniting with FortiGates to **automatically quarantine** attacks

HIGHLIGHTS

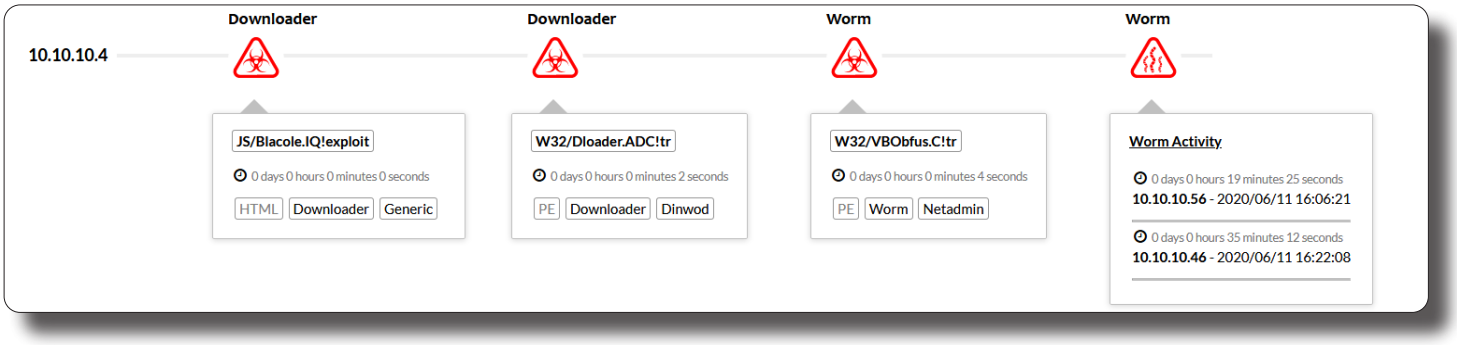
Virtual Security Analyst™

Responsibilities include:

- **Identifying and Classifying Attack Scenarios –** determines malware attack scenarios with chain-on-infection and big picture analysis
- **Investigating the Source of Attack –** tracking the original source of infection with timestamps
- **Emulating as a FortiGuard Malware Analyst –** scientifically determine the type of malware based on an evolving Neural Networks that constantly learns and matures over time and experience
- **Outbreak Search –** searches networks for traces of malware outbreaks based on hashes and similar variants on network

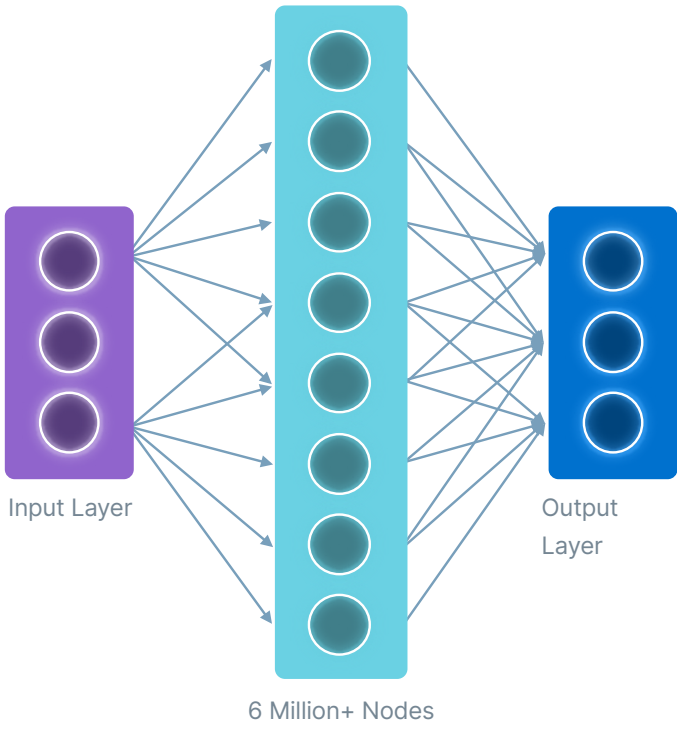
99.9%	<100 ms
Detection Rate*	Sub-Second Detection
10G	100K
Network Throughput	Files / hour
20+	200 Billion
Attack Scenarios	Exposed Features

Tracing the Source of a Worm Attack



State-of-the-Art Artificial Neural Network (ANN)

- The state-of-the-art ANN is pre-trained in FortiGuard labs with 20M+ clean and malicious files and further learning is done on premise; updates of the ANN model are available from FortiGuard network to ensure customers are protected against the latest threats
- Responsible for classifying malware types into 20+ attack scenarios and AI-based engine for tracing source of attacks, emulating how a human brain operates
- AI-driven breach protection with multi-task threat learning framework to incorporate complex security needs into a single high-performance network security appliance
- Using Machine Learning and Neural Network technology, the Multilayer Detection approach provides deep machine learning capabilities before post infection damages are caused by the modern day AI-powered cyber attacks
- Pre-trained in FortiGuard labs with millions of known clean and malicious samples forming billions of clean and malicious features, which is used to scientifically decide malware and attack type specific to your organizations' security environment



FEATURES

Core Engine

- Patent-pending malware analysis with multiple artificial neural networks
- Pre-trained with millions of malware features
- Scenario-based engine to locate patient zero
- Outbreak search engine (hash, virus family)
- Similarity engine to look for malware and its variants on the network
- File IOC (Indicator of Compromise) analysis
- MITRE ATT&CK Malware mapping
- Allow/Deny List

Malware Classification

- AI-driven Security Attack Scenarios: Industroyer, Wiper, Downloader, Redirector, Dropper, Ransomware, Worm, Password Stealer, Rootkit, Banking Trojan, InfoStealer, Exploit, Clicker, Virus, Application, CoinMiner, DoS, BackDoor, WebShell, Search Engine Poisoning, Proxy, Trojan, Phishing, Fileless and more

Deployment Modes

- Sniffer, integrated and inline blocking (with FortiGates), manual upload/REST API, and ICAP
- ICAP Server: FortiAI
  ICAP clients: FortiGate v6.4.0+, FortiWeb v6.3.11+, and third party such as Squid

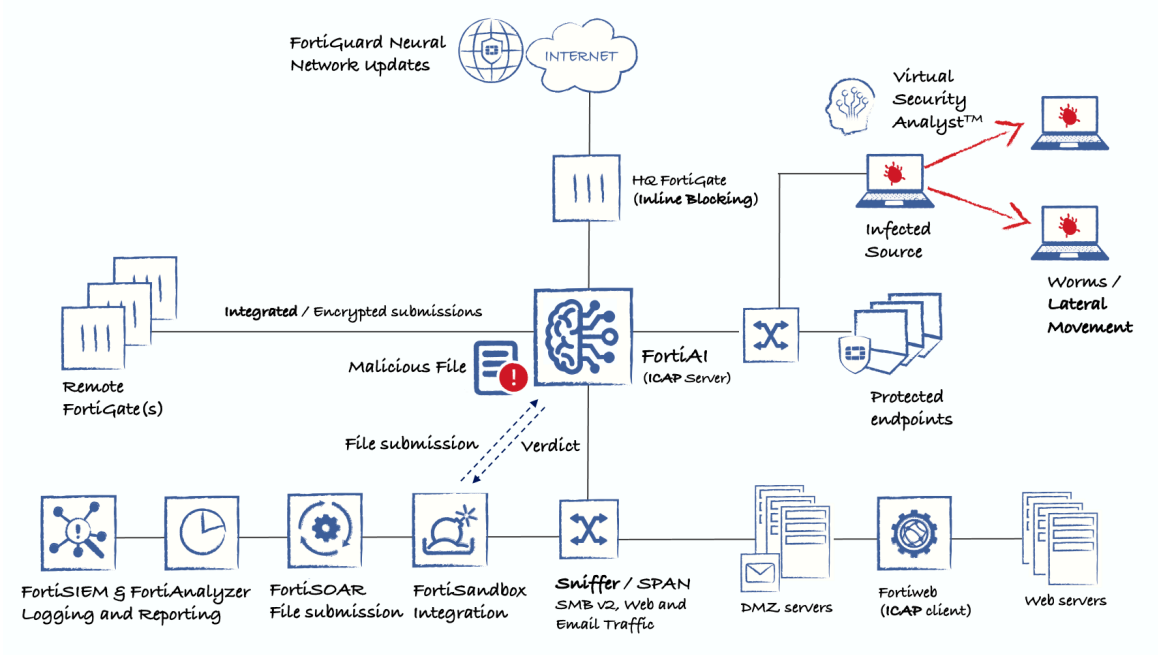
File Types and Protocols

- 32bit and 64bit Portable Executables (PE) files including DLLs and self-extracting ZIP files
- Web based, text, and PE files such as HTML, PDF, JS, VBS, VBA, ELF, HWP (Hancom), 32 & 64bits PE files including DLLs, MSOFFICE, DEX, PHP, XML, POWERSHELL, Archive files including ZIP, TAR, XZ, GZIP, BZIP, BZIP2, RAR, LZH, LZW, ARJ, CAB, and 7Z

Systems and Integration

- Log and Report: SYSLOG support , MD5/SHA1/SHA256 hashes, VSATM report in JSON, STIX2, STIX v2, and PDF format, URLs, VDOM and timestamps of attacks
- Networking: Static route and IPv4 support
- Systems: Role based Administration Support (RBAC)
- FortiGate Security Fabric (v7.0.0+) with inline blocking (v7.0.1+)
- FortiSOAR Connector (for files submission)
- FortiAnalyzer v7.0.1+ Log and View
- FortiSIEM v6.3.0+ Parser, Log, and Dashboard
- Third-party: SYSLOG, REST API, and ICAP

DEPLOYMENT



SPECIFICATIONS

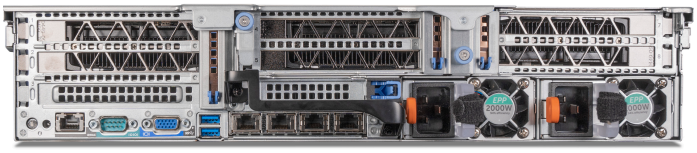
	FortiAI-3500F
Hardware Specifications	
Form Factor	2 RU Rackmount
Total Interfaces	2 × 10GE RJ45 (10/100/1000), 1 x GE RJ45 IPMI, 1 x DB9 Console
Storage Capacity	2 × 3.84TB SSD, Total 7.68TB
Default RAID level (RAID software)	1
Removable Hard Drives	✓
Redundant Hot Swappable Power Supplies	✓
Custom GPUs for ANN Acceleration	✓
System Performance	
Throughput (files per hour)[1]	100,000
Sub-second verdicts	✓
Sniffer Throughput	Line rate 10G
Dimensions	
Height x Width x Length (inches)	3.41in x 18.98in (w/ handle) x 29.58in (w/ bezel), 3.41in x 17.09in (w/o handle) x 29.04in (w/o bezel)
Height x Width x Length (mm)	86.8mm x 482mm (w/ handle) x 751.34mm (w/ bezel), 86.8mm x 434mm (w/o handle) x 737.5mm (w/o bezel)
Weight	68.34lbs (31kg)
Environment	
AC Power Supply	100-240 VAC, 60-50 Hz
Power Consumption (Average / Maximum)	1390W / 1668W
Heat Dissipation	6824 BTU/h
Operating Temperature	10°C to 35°C (50°F to 95°F) with no direct sunlight on the equipment
Storage Temperature	–40°C to 65°C (–40°F to 149°F)
Humidity	Storage: 5% to 95% RH with 33°C (91°F) maximum dew point. Atmosphere must be non-condensing at all times. Operation: 10% to 80% relative humidity with 29°C (84.2°F)
Operating Altitude	Up to 7,400 ft (2,250 m)
Compliance	
Safety Certifications	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB

[1] Combined real-world throughput based on 90/10 Non-PE/PE files

	FortiAI-VM16	FortiAI-VM32
Technical Specifications		
vCPU Support (Recommended)	16	32
Memory Support (Minimum / Recommended)	128GB / 256GB	
Recommended Storage	1TB to 8TB	
Default RAID level (RAID software)	Hypervisor Hardware Dependent	
System Performance		
Throughput (files per hour)[2]	14,000	22,000
Sub-second verdicts	✓	✓
Sniffer Throughput	Hypervisor Hardware Dependent	
Hypervisor Support	ESXi 6.7 U2+ and KVM	

FortiAI-3500F Front

FortiAI-3500F Rear



[2] Throughput in both the FAI-3500F device and VM

ORDER INFORMATION

Product	SKU	Description
FortiAI 3500F	FAI-3500F	FortiAI-3500F appliance for 0day/Malware Detection, based on Artificial Neural Network (ANN) technology. 2 × 10Gb GE Copper (supports 10/1000/10000 without transceivers) Note: FAI-3500F ships with 2 × 3.84TB SSD by default
FortiAI-3500F Hardware Bundle	FAI-3500F-BDL-228-DD	FortiAI-3500F bundle - Hardware plus 24×7 FortiCare and FortiGuard Neural Networks engine updates & baseline
FortiAI-VM Subscription License with Bundle	FC3-10-AIVMS-238-02-DD	Subscriptions license for FortiAI-VM (16 CPU) with 24×7 FortiCare plus FortiGuard Neural Networks engine updates & baseline
	FC4-10-AIVMS-238-02-DD	Subscriptions license for FortiAI-VM (32 CPU) with 24×7 FortiCare plus FortiGuard Neural Networks engine updates & baseline
FortiCare and Updates	FC-10-AI3K5-228-02-DD	24×7 FortiCare plus FortiGuard Neural Networks engine updates & baseline
3.84TB 2.5" SATA SSD with Tray	SP-DFAI-3T	3.84TB 2.5" SATA SSD with tray for FAI-3500F

FORTINET

www.fortinet.com