DATA SHEET

FortiNDR

Available in:

Appliance

Virtual Machine

Network Detection and Response with Virtual Security Analyst™

FortiNDR 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 threats including those well camouflaged. FortiNDR employs patent-pending* **Deep Neural Networks based on Advanced AI and Artificial Neural Network** to provide sub-second investigation by harnessing deep learning technologies that assist you in an automated response to remediate different breeds of attacks. **FortiNDR significantly reduces the time** to identify network anomalies and malicous content on your network and mitigate with Fortinet Security Fabric and third Party integration.

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

High volume of north-south and east-west traffic is processed in data centre using ML and advance analytics to identify and respond to breaches

AI-Powered Detection and Response for Cyber Attacks

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

ML-based Malware

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

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

Key Features

- **Detect network anomalies** where traditional security solutions fail
- **Automate and manually respond** for quarantine and control
- Mimic experienced security analyst for outbreak, anomalies, and malware detection, processing large volume of network data
- Reduce malware detection and investigation time from minutes to **sub-second verdict**
- Provide **on-premises learning** to reduce false positives by analyzing organizational-specific traffic and adapting to newly disguised threats
- Integrate into Fortinet's Security Fabric by uniting with FortiGates and others to **automatically quarantine attacks**
- Analyze zero days scientifically including fileless threats and classify them into **20+ malware attack scenarios**

HIGHLIGHTS

Network Detection Response

Responsibilities

DETECT

- Detect encrypted attack, malicious web campaigns, weaker ciphers, vulnerable protocols, IP and DNS-based botnet attacks with advanced analytics
- Profile network traffic with ML models to identify anomalies with user feedback mechanism
- Detect malicious files in sub-seconds through neural network analysis including NFS file shares

RESPOND

- Integrate Fortinet Security Fabric and third party (via API) with FortiGate inline blocking, FortiSwitch/FortiNAC quarantine, FortiAnalyzer, and FortiSOAR

Virtual Security Analyst™

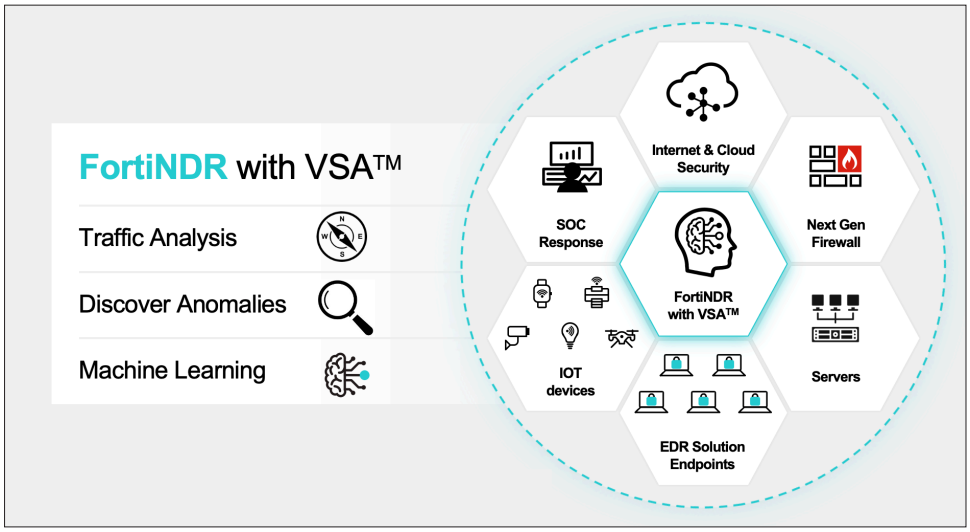
Responsibilities

ANALYZE

- Identify and classify attack scenarios that determines malware attacks with chain-on-infection and big picture analyses
- Investigate the attack source by tracking the original source of infection with time stamps
- Emulate a FortiGuard malware analyst and scientifically determine the type of malware based on an evolving neural networks that constantly learns and matures over time and experience

SECURE

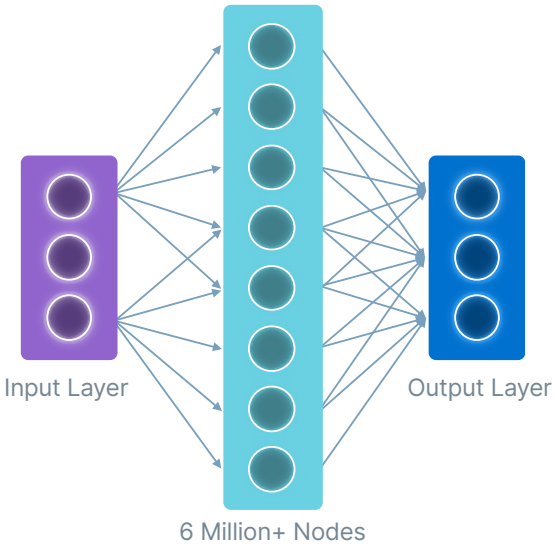
- Search for outbreaks on networks and look for traces of malware based on hashes and similar variants



FortiNDR can be placed in network to detect threats among high volume of network and file transfers, to strengthen threat detection, and tosecure network segments. Assisting security operations by mimicking human analysis experience as well as tracing outbreaks. Coupled with mitigation via Fortinet Security Fabric as well as third party solution based on APIs.

State-of-the-Art Artificial Neural Network (ANN) for Malware Detection

- The state-of-the-art ANN is pre-trained in FortiGuard labs with 20M+ clean and malicious files and further learning is done on premises; 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
- 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

Deployment Modes

- Sniffer, integrated and inline blocking (with FortiGates), and manual upload/REST API
- ICAP Server: FortiNDR
  ICAP clients: FortiGate v6.4.0+, FortiProxy v7.0, FortiWeb v6.3.11+, and third party such as Squid

Malware 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

File Types and Protocols

NDR engine: common protocols such as TCP, UDP, ICMP, ICMP6, TLS, HTTP, SMB, SMTP, SSH, FTP, POP3, DNS, IRC, IMAP, RTSP, RPC, SIP, RDP, SNMP, MYSQL, MSSQL, PGSQL, and their behaviors

File-based analyses: 32 bit and 64 bit PE - Web based, text, and PE files such as EXE, PDF, MSOFFICE, DEX, HTML, ELF, ZIP, VBS, VBA, JS, Hangul_Office, TAR, XZ, GZIP, BZIP, BZIP2, RAR, LZH, LZW,ARJ, CAB, _7Z, PHP, XML, POWERSHELL, BAT, HTA, UPX, ACTIVEMIME, MIME, HLP, BASE64, BINHEX, UUE, FSG, ASPACK, GENSCRIPT, SHELLSCRIPT, PERLSCRIPT, MSC, PETITE, ACCESS, SIS, HOSTS, NSIS, SISX, INF, E32IMAGE, FATMACH, CPIO, AUTOIT, MSOFFICEX, OPENOFFICE, TNEF, SWF, UNICODE, PYARCH, EGG, RTF, DLL, DOC, XLS, PPT, DOCX, XLSX, PPTX, LNK, KGB, Z, ACE, JAR, APK, MSI, MACH_O, DMG, DOTNET, XAR, CHM, ISO, CRX, INNO, THMX, FLAC, XXE, WORDML, WORDBASIC, OTF, WOFF, VSDX, EMF, DAA, GPG, PYTHON, CSS, AUTOITSCRIPT, RPM, EML, REGISTRY, PFILE, CEF, PRC, CLASS, JAD, COD, JPEG, GIF, TIFF, PNG, BMP, MPEG, MOV, MP3, WMA, WAV, AVI, RM, TOR, HIBUN

Systems and Integration

Systems

- LDAP / RADIUS RBAC admin profiles, SYSLOG, STIX/JSON for malware, and IPv4 static route support

Devices Input

- FortiGate (5.6+), FortiMail (v7.2+), FortiSandbox (v4.0.1+), FortiSOAR (connector), FortiProxy (v7.0+) and FortiWeb (via ICAP), and third party ICAP clients

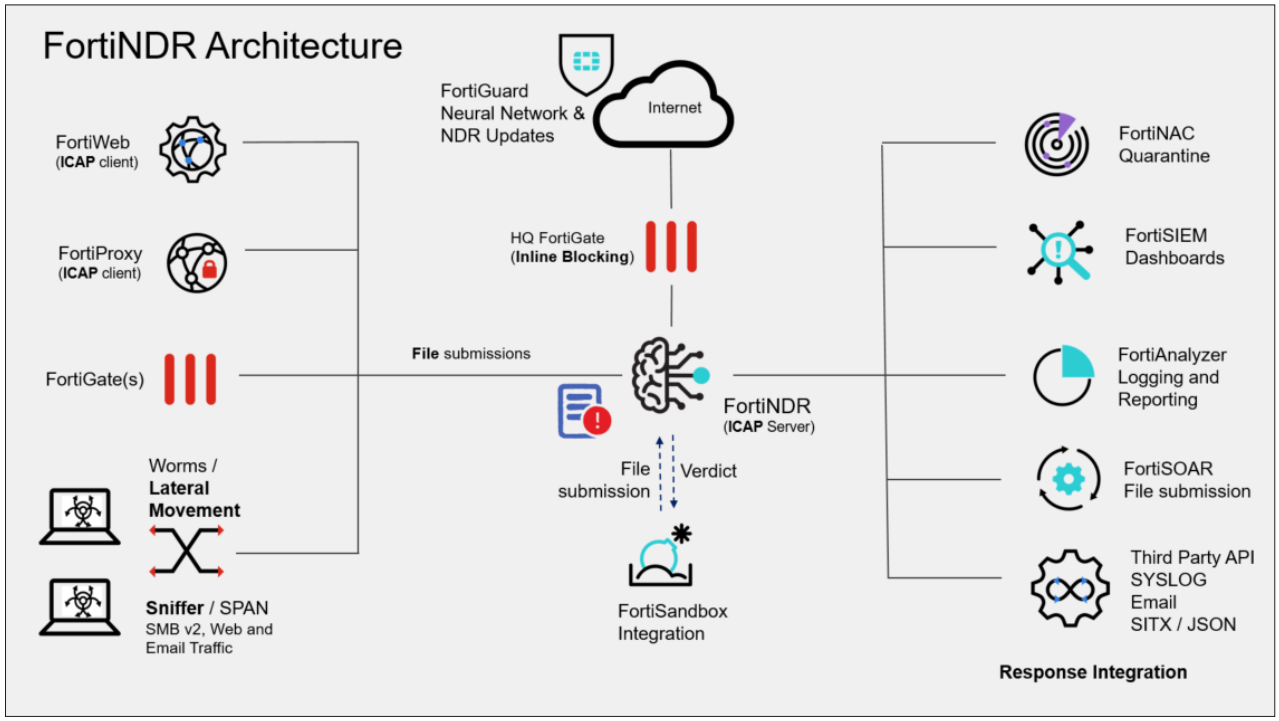
Response

- FortiGate (v7), FortiNAC and FortiSwitch quarantine (via FortiLink), FortiSOAR (via syslog), and third Party API call

Log and Report

- Local logs with STIX/JSON output (malware), FortiAnalyzer, and FortiSIEM support

DEPLOYMENT



SPECIFICATIONS

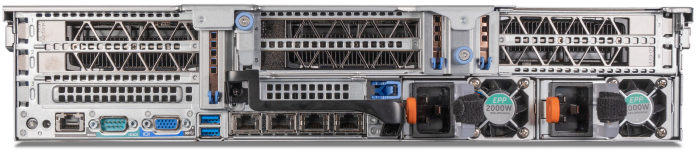
	FortiNDR-3500F
Hardware Specifications	
Form Factor	2 RU Rackmount
Total Interfaces	2× 10GE RJ45 (10/100/1000), 1x GE RJ45 IPMI, 1x DB9 Console
Storage Capacity	2× 3.84 TB SSD, Total 7.68 TB
Default RAID level (RAID software)	1
Removable Hard Drives	✓
Redundant Hot Swappable Power Supplies	✓
Custom GPUs for ANN Acceleration	✓
System Performance	
NDR Sniffer Throughput[1]	5 Gbps
Malware Analysis Throughput (files per hour)[2]	100 000
Sub-second verdicts	✓
Dimensions	
Height x Width x Length (inches)	3.41 in x 18.98 in (w/ handle) x 29.58 in (w/ bezel), 3.41 in x 17.09 in (w/o handle) x 29.04 in (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	68.34 lbs (31 kg)
Environment	
AC Power Supply	100-240 VAC, 60-50 Hz
Power Consumption (Average / Maximum)	1390 W / 1668 W
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 7400 ft (2250 m)
Compliance	
Safety Certifications	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB

	FortiNDR-VM16	FortiNDR-VM32
Technical Specifications		
vCPU Support (Recommended)	16	32
Memory Support (Minimum / Recommended)	128 GB / 256 GB	
Recommended Storage	1 TB to 8 TB	
Default RAID level (RAID software)	Hypervisor Hardware Dependent	
NDR Sniffer Throughput[1]	Hypervisor Hardware Dependent	
Malware Analysis Throughput (files per hour)[3]	14 000	22 000
Sub-second verdicts	✓	
Hypervisor Support	ESXi 6.7 U2+ and KVM	

[1] Based on ideal lab condition
[2] Combined real world throughput based on 90/10 Non-PE/PE files
[3] Based on standard modern server without GPU acceleration
Cloud Support (BYOL), "AWS" for both VM16 and VM32

FortiNDR-3500F Front

FortiNDR-3500F Rear



ORDER INFORMATION

Product	SKU	Description
FortiNDR 3500F	FAI-3500F	FortiNDR-3500F appliance for 0day/Threat Detection, based on NDR and ANN updates. 2× 10Gb GE Copper (supports 10/1000/10 000 without transceivers). Note: FAI-3500F ships with 2× 3.84TB SSD by default.
FortiNDR-3500F Hardware Bundle	FAI-3500F-BDL-228-DD	FortiNDR-3500F bundle - Hardware plus 24×7 FortiCare and NDR and ANN updates and baseline.
FortiNDR-VM Subscription License with Bundle	FC3-10-AIVMS-238-02-DD	Subscriptions license for FortiNDR-VM (16 CPU) with 24×7 FortiCare plus NDR and ANN updates and baseline.
	FC4-10-AIVMS-238-02-DD	Subscriptions license for FortiNDR-VM (32 CPU) with 24×7 FortiCare plus NDR and ANN updates and baseline.
FortiCare and Updates	FC-10-AI3K5-228-02-DD	24×7 FortiCare plus FortiGuard Neural Networks engine updates and baseline.
3.84TB 2.5" SATA SSD with Tray	SP-DFAI-3T	3.84TB 2.5" SATA SSD with tray for FortiNDR-3500F.

FORTINET

www.fortinet.com