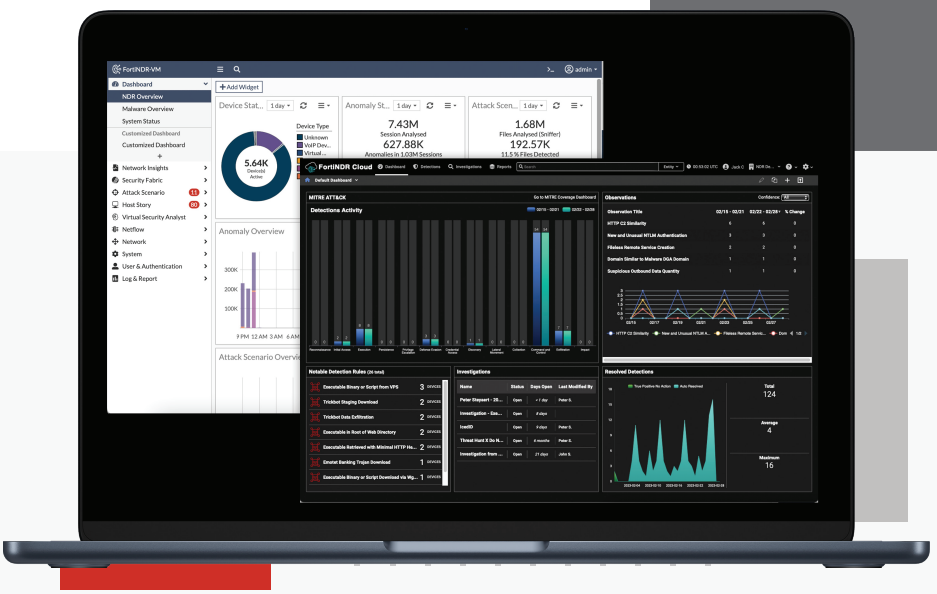
FortiNDR 및 FortiNDR Cloud



하이라이트

- 강력한 AI로 사이버 공격을 발견하고 대응
- 탐지 집계 메타데이터 발견
- 기존의 탐지가 작동하지 않는 경우 턴키 보안 활용
- SOC 기술 및 리소스 부족 충당

네트워크 탐지 및 대응

FortiNDR 및 FortiNDR Cloud(일명, ThreatINSIGHT)는 AI 중심적 보안 침해 보호 기술의 미래를 상징합니다. 인력이 부족한 보안 관제 센터(SoC) 팀이 훈련된 Virtual Security Analyst™ 및 은밀히 은폐된 위협까지 모두 식별, 분류 및 대응할 수 있도록 도와주는 "가이드형 SaaS"를 통해 지능적 지속 위협 등의 다양한 위협을 방어하도록 설계되었습니다.

현대적 SoC에서 위협 탐지에 메타데이터를 사용하는 것은 필수입니다. 지도 및 비지도 머신 러닝을 메타데이터에 적용할 수 있으며, 특히 데이터 센터에 있는 이스트-웨스트 데이터에 적용하여 위협을 식별할 수 있습니다.

FortiNDR은 네트워크에서 네트워크의 이상과 악성 콘텐츠를 찾는 시간을 단축하고, Fortinet 보안 패브릭과 타사 통합으로 이를 완화합니다.

하이라이트

사용 가능한 분야

어플라이언스

VM

클라우드
SaaS

퍼블릭
클라우드

주요 기능[1]

- 기존 보안 솔루션에 장애 발생 시 네트워크 이상 탐지
- 과거의 트렌드와 365일 데이터로 위협 조사
- 가이드형 플레이북으로 적대 세력 헌팅
- 격리 및 제어를 위한 자동화 및 수동 대응
- 확산, 이상 및 멀웨어 탐지를 위한 숙련된 보안 분석가를 모방하여 대량 네트워크 데이터 처리
- 멀웨어 탐지 및 조사 시간을 분 단위에서 초 단위로 단축[2]
- 온프레미스 학습을 통해 기업의 특정한 트래픽을 분석하고 새롭게 위장한 위협에 적응해 오탐지 감소
- FortiGate 등과의 결합을 통해 포티넷의 시큐리티 패브릭과 통합하여 공격을 자동으로 격리
- 파일에 기반하지 않은 위협을 포함한 제로데이 위협을 과학적으로 분석하고 이를 20가지 이상의 멀웨어 공격 시나리오로 분류

1 다음 페이지의 FortiNDR 및 FortiNDR Cloud의 기능 비교를 참조하세요.
2 특허 출원 #U.S.16/053,479

기본 역량

숙련된 SOC 분석가의 부족

사이버 보안, 특히 위협 분석, 확산 조사 및 멀웨어 연구에서의 경험은 가장 획득하기 어렵습니다. FortiNDR은 FortiNDR Cloud와 함께 **Virtual Security Analyst™** 및 **가이드형** 기술 성공 관리자(TSM)를 제공합니다.

Breach Prevention

ML과 서명 기반을 사용하여 높은 신뢰도로 보안 침해를 식별하며, 여기에는 공격에 대한 데이터 보강도 포함됩니다.

사이버 공격에 대한 AI 기반 탐지 및 대응

혁신적인 위협 행위자는 SOC 방어를 압도하거나 슬그머니 통과하도록 설계된 자동 공격을 통해 사이버 보안을 방해합니다.

ML 기반 트래픽 프로파일링 및 멀웨어 탐지

교묘하게 설계된 사이버 위협은 멀웨어 탐지로부터 숨어 기존 보안 제어를 우회하도록 설계되어 있습니다.

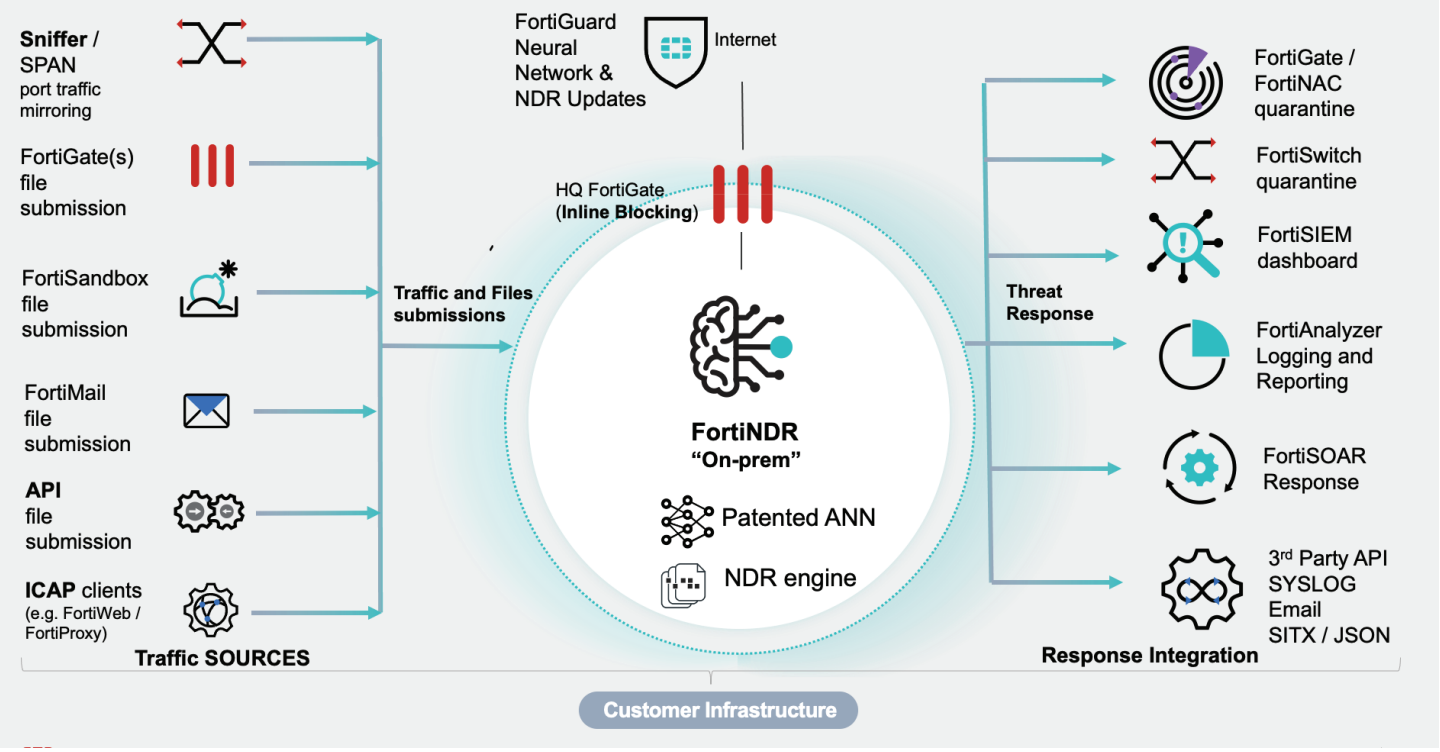
하이라이트

특징	FortiNDR(HW/VM)	FortiNDR Cloud
배포	온프레미스	SaaS
보안 분석가	Virtual Security Analyst™	가이드형 SaaS, TSM(기술 성공 관리자) 포함
데이터 스토리지 위치	온프레미스	클라우드 기반(US)
데이터 보관	처리량/디스크 종속적	365일
조사/위협 헌팅	보안 침해 검색	가이드형 플레이북 및 병렬 헌팅
Netflow/IPFIX 지원	예	—
대량 멀웨어 스캔 / NFS 스캔	예 ANN1 온프레미스 학습 포함	해시 검색
MITRE ATT&CK 프레임워크 매핑	MITRE ATT&CK 프레임워크에 매핑된 멀웨어	MITRE ATT&CK 프레임워크에 매핑된 탐지
대응 통합	Fortinet 보안 패브릭 타사 API (Rest) 신호가 포함된 MetaStream	
센서	하드웨어: FortiNDR-1000F, FortiNDR-3500F VM16 / VM32 (ESXi / KVM) AWS / Azure / GCP / Alibaba	하드웨어: FortiNDR Cloud-900F (대형 센서) 하드웨어: FortiNDR Cloud-500F (소형 센서) 가상 센서 (AWS / Azure / ESXi / KVM)
FortiGuard Labs Threat Research	✓	✓

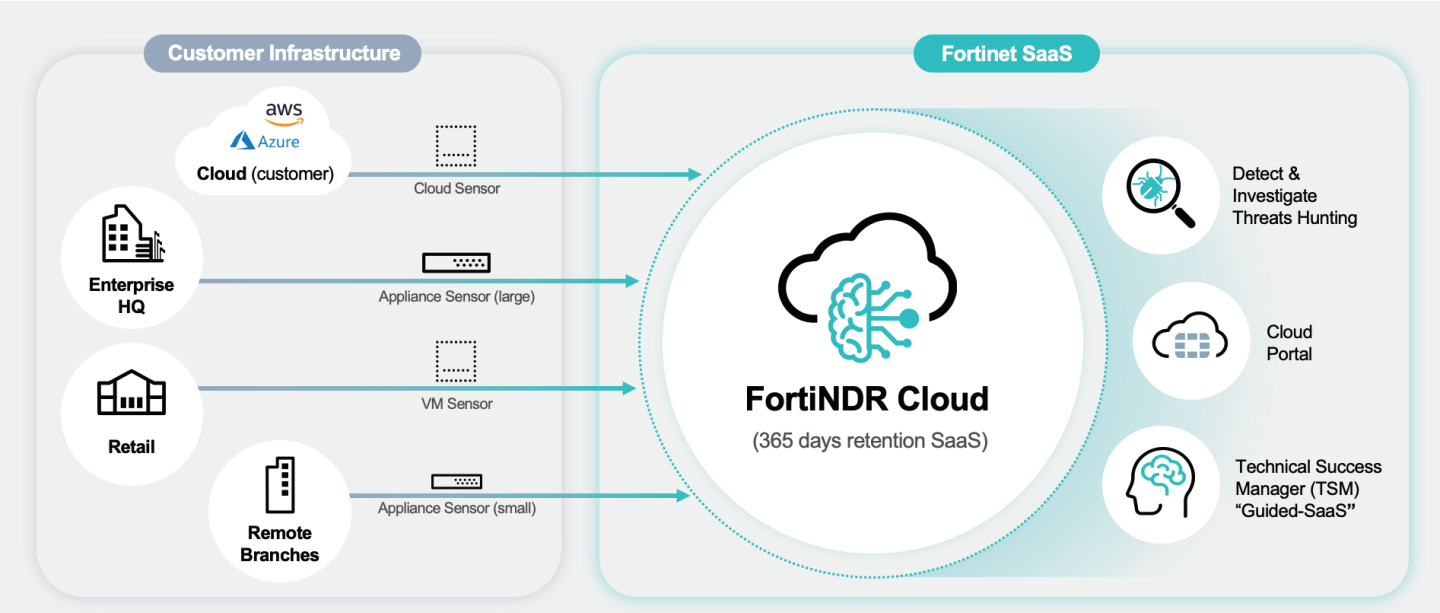
1. 인공 신경망

배포

FortiNDR (온프레미스) 아키텍처 및 통합



FortiNDR 클라우드 아키텍처 및 배포



사양

카테고리	FortiNDR-1000F	FortiNDR-3500F	FNDR VM 16	FNDR VM 32	FNDR Cloud 500F 소형 센서	FNDR Cloud 900F 대형 센서	FNDR Cloud 가상 센서
배포							
Sniffer / SPAN / 802.1q 지원	✓	✓	✓	✓	✓	✓	✓
클라우드 기반 센서 + SaaS 포털	—	—	—	—	✓	✓	✓
통합성 (패브릭 기기 포함) 및 ICAP	✓	✓	✓	✓	—	—	—
하이퍼바이저 지원	—	—	ESXi 6.7 U2+, KVM	ESXi 6.7 U2+, KVM	—	—	ESXi6.7 U2+, KVM
하드웨어 사양							
폼팩터	2 RU 랙마운트	2 RU 랙마운트	—	—	—	—	—
총 인터페이스	2x 10/100/1000 RJ45 포트, 4x 10G SFP+, 1 x RJ45 콘솔	4x 10GbE SFP+, 2x 10GE 구리 (10/100/1000), 2x 1G 구리, 1x DB9 콘솔	4x 가상 인터페이스	4x 가상 인터페이스	1 x 1G 구리, 2 x 10G SFP+, 2 x 10G 구리	1 x 1G 구리, 2 x 10G SFP+, 2 x 10G 구리	1 mgmt + 최소 1 TAP
Sniffer 인터페이스	3 (3 x 섬유 10G SFP+)*	5 (1 x 구리 10G, 4 x 10G 섬유 SFP+)*	1 x vNIC	1 x vNIC	5 (1 x 1G 구리, 2 x 10G SFP+, 2 x 10G 구리)	5 (1 x 1G 구리, 2 x 10G SFP+, 2 x 10G 구리)	최소 1 x vNIC 최대 3 x vNIC
트랜시버 포함	별매[2]	별매	—	—	2x 10G 멀티모드	4x 10G 멀티모드	—
저장 용량	2 x 7.68 TB (RAID 1) 총 7.68 TB (RAID 1)	8 x 3.84TB SSD, 총 15.36 TB (RAID 10)	1-8TB	1-8TB	890 GB	890 GB	100 (최소) - 300 GB (권장)
기본 RAID 레벨 (RAID 소프트웨어)	1	10	하이퍼바이저 종속적	하이퍼바이저 종속적	10	10	하이퍼바이저 종속적
이동식 하드 드라이브	✓	✓	—	—	예	예	—
예비 핫스왑 전원	✓	✓	—	—	예	예	—
ANN 가속화를 위한 맞춤형 GPU	—	✓	—	—	—	—	—
기술 사양							
vCPU 지원 (권장)	—	—	16	32	—	—	16
메모리 지원 (최소 / 권장)	—	—	32 GB/128 GB	64 GB/256 GB	—	—	16 GB/32 GB
권장 보관	—	—	1TB~8TB	1TB~8TB	—	—	—
시스템 성능							
NDR Sniffer 처리량	10 Gbps/ 10 Gbps (HTTP/ 엔터프라이즈 믹스) - 단일 포트 스니퍼 20 Gbps / 20 Gbps (HTTP/ P/ 엔터프라이즈 믹스) - 듀얼 포트 스니퍼	10 Gbps/ 9.5 Gbps (HTTP/ 엔터프라이즈 믹스) - 단일 포트 스니퍼 20 Gbps/ 13 Gbps (HTTP/ 엔터프라이즈 믹스) - 듀얼 포트 스니퍼	하이퍼바이저 종속적	하이퍼바이저 종속적	모든 포트에서 2 Gbps (메타데이터 처리)	모든 포트에서 10 Gbps (메타데이터 처리)	하이퍼바이저 종속적
멀웨어 분석 처리량 (파일/시간)[1]	시간당 파일 17만 개	시간당 파일 13만 개	40,000	80,000	해시 검색 (VT) 대상	해시 검색 (VT) 대상	해시 검색 (VT) 대상
멀웨어 분류	26개 카테고리	26개 카테고리	26개 카테고리	26개 카테고리	—	—	—

1) 10:1 Non-PE/PE 파일에 기반하여 실제 처리량을 결합했습니다.
2) FNR-1000F에 구리가 필요한 경우(예: mgmt 또는 sniffer), 고객은 Fortinet FN-TRAN-GC으로 1G를 사용할 수 있습니다.
FNR-1000F에 10G 구리가 필요한 경우, 고객은 https://www.fs.com/products/89577.html에서 E10GSFPT를 구매해야 합니다. Fortinet FN-TRAN-SFP+SR 및 FN-TRAN-SFP+LR은 NDR-1000F 및 NDR-3500F 플랫폼에서도 지원됩니다.

사양

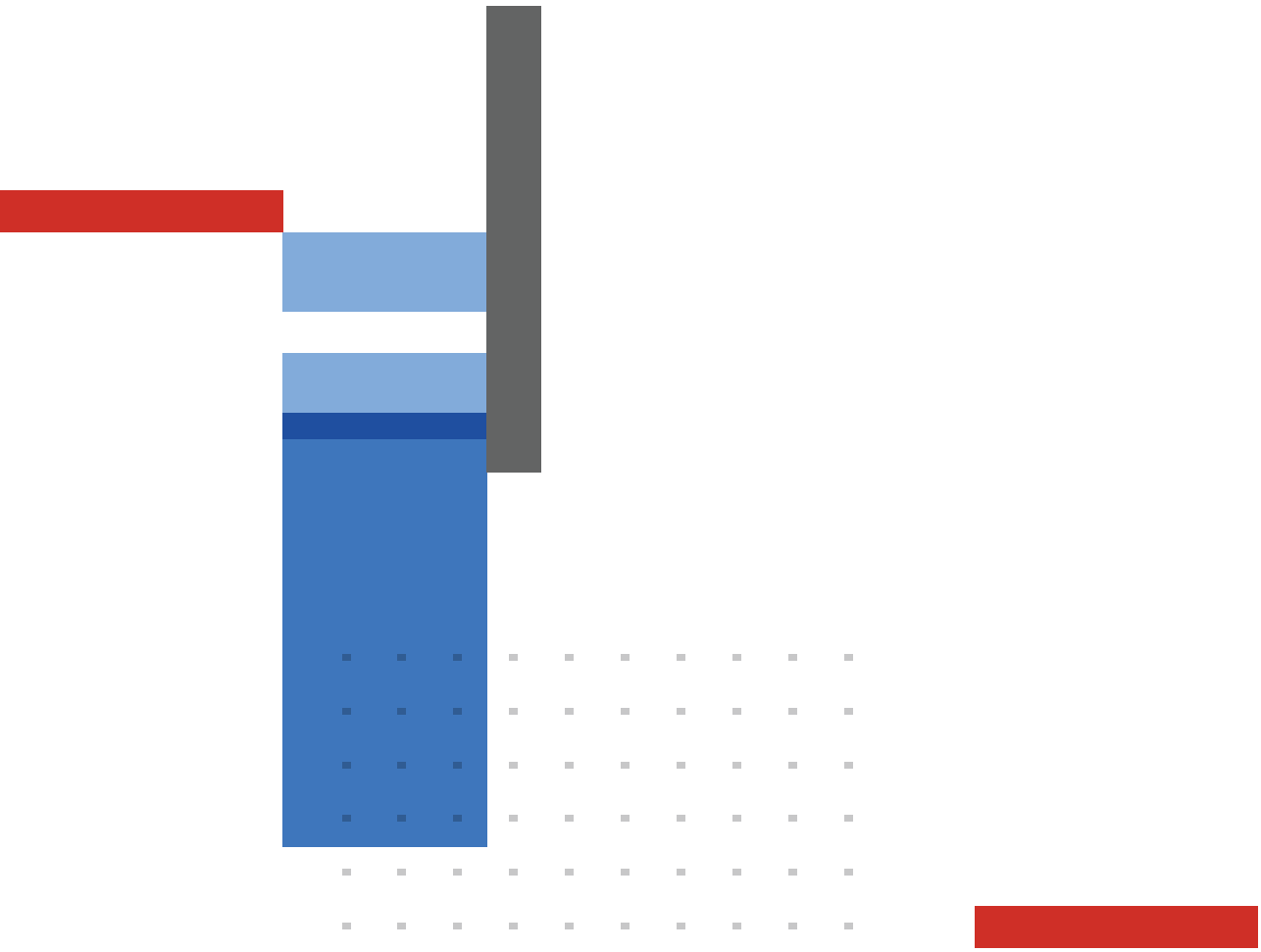
카테고리	FortiNDR-1000F	FortiNDR-3500F	FNDR VM 16	FNDR VM 32	FNDR Cloud 500F 소형 센서	FNDR Cloud 900F 대형 센서	FNDR Cloud 가상 센서
규격							
높이 x 너비 x 길이(mm)	88.9 mm x 444.5 mm x 574.04 mm	86.8 mm x 482 mm (손잡이 포함) x 751.34 mm (베젤 포함) 86.8 mm x 434 mm (손잡이 미포함) x 737.5 mm (베젤 미포함)	—	—	42.8 mm. x 482 mm (손잡이 포함) x 757.75 mm (베젤 포함) 42.8mm x 434 mm (손잡이 미포함) x 743.91 mm (베젤 미포함)	42.8 mm. x 482 mm (손잡이 포함) x 757.75 mm (베젤 포함) 42.8mm x 434 mm (손잡이 미포함) x 743.91 mm (베젤 미포함)	—
무게	34.6 lbs (16 kg)	68.34lbs(31kg)	—	—	25.9 kg	25.9 kg	—
환경							
AC 전원공급장치	100-240 VAC, 60-50 Hz	100-240 VAC, 60-50 Hz	—	—	100-240 VAC, 60-50 Hz	100-240 VAC, 60-50 Hz	—
전력 소비 (평균/최대)	163 W (유휴) 345 W (완전 부하)	1390 W/1668 W	—	—	276 W/390 W	409 W/619 W	—
방열	1207.5 BTU/h	6,824BTU/h	—	—	2891 BTU/h	2891 BTU/h	—
작동 온도	0°C~40°C (32°F ~104°F) 직사광선을 피해서 장비 보관	10°C~35°C (50°F~95°F) 직사광선을 피해서 장비 보관	—	—	10°C~35°C(50°F~95°F) 직사광선을 피해서 장비 보관	10°C~35°C(50°F~95°F) 직사광선을 피해서 장비 보관	—
보관 온도	-20°C~70°C (-4°F~158°F)	-40°C~65°C (-40°F~149°F)	—	—	-40°C~65°C (-40°F~149°F)	-40°C~65°C (-40°F~149°F)	—
습도	보관: 5%~90% 비응축	보관: 5%~95% RH, 33°C (91°F) 최대 이슬점. 대기는 항상 비응축 상태여야 합니다. 작동: 10%~80% 상대 습도, 29°C (84.2°F)	—	—	보관: 5%~95% RH, 33°C (91°F) 최대 이슬점. 대기는 항상 비응축 상태여야 합니다. 작동: 10%~80% 상대 습도, 29°C (84.2°F) 최대 이슬점.	보관: 5%~95% RH, 33°C (91°F) 최대 이슬점. 대기는 항상 비응축 상태여야 합니다. 작동: 10%~80% 상대 습도, 29°C (84.2°F) 최대 이슬점.	—
작동 고도	최대 16 404 ft (5000 m)	최고 7,400피트(2250 m)	—	—	최대 10 000 ft (3048 m)	최대 10 000 ft (3048 m)	—
규정 준수							
안전 인증	FCC Part 15 Class A, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/ cUL, CB	—	—	FCC, ISED, CE, RCM, VCCI, BSMI (Class A), UL/cUL, CB	FCC, ISED, CE, RCM, VCCI, BSMI (Class A), UL/cUL, CB	—

주문 정보

FORTINDR 어플라이언스 및 VM		
제품	**SKU**	**설명**
FortiNDR-1000F	FNR-1000F	인공 신경망(ANN) 기술에 기반한 네트워크 이상 및 제로데이/멀웨어 탐지를 위한 어플라이언스. 4x 10GbE SFP+, 2 x 1기가비트 이더넷 연결(관리). Netflow는 별도로 주문해야 합니다.
FortiNDR-1000F용 Netflow	FC-10-AI1KF-588-02-DD	FortiNDR-1000F에 Netflow를 지원합니다
FortiNDR-1000F 하드웨어 번들	FNR-1000F-BDL-331-DD	FortiNDR-1000F 하드웨어 + FortiCare Premium, NDR 및 ANN 엔진 업데이트 및 기준치. 인공 신경망(ANN) 기술에 기반한 네트워크 이상 및 제로데이/멀웨어 탐지를 위한 FortiNDR-1000F 어플라이언스. 4x 10GbE SFP+, 2x 10Gb GE 구리(트랜시버 없이 10/1000/10000 지원), 2x 1 기가비트 이더넷 연결(관리). Netflow는 별도로 주문해야 합니다.
FortiNDR-1000F 갱신	FC-10-AI1KF-331-02-DD	FortiCare Premium, NDR 및 ANN 엔진 업데이트 및 기준치.
제품	**SKU**	**설명**
FortiNDR 3500F	FNR-3500F	인공 신경망(ANN) 기술에 기반한 네트워크 이상 및 제로데이/멀웨어 탐지를 위한 FortiNDR-3500F 어플라이언스. 4x 10GbE SFP+, 2x 10Gb GE 구리(트랜시버 없이 10/1000/10 000 지원), 2x 1 기가비트 이더넷 연결(관리). 트랜시버는 별도로 주문합니다.
FortiNDR-3500F용 Netflow	FC-10-AI3K5-588-02-DD	FortiNDR-3500F에 Netflow를 지원합니다
FortiNDR-3500F 하드웨어 번들	FNR-3500F-BDL-331-DD	FortiNDR-3500F 번들 - 하드웨어 + 상시 FortiCare 및 NDR 및 ANN 업데이트 및 기준치 제공.
제품	**SKU**	**설명**
FortiNDR-VM 구독 라이선스, 번들 포함	FC3-10-AIVMS-461-02-DD	FortiNDR-VM(16 CPU) 구독 라이선스, 상시 FortiCare + NDR 및 ANN 업데이트 및 기준치.
	FC4-10-AIVMS-461-02-DD	FortiNDR-VM(32 CPU) 구독 라이선스, 상시 FortiCare + NDR 및 ANN 업데이트 및 기준치.
VM16용 Netflow	FC3-10-AIVMS-588-02-DD	FortiNDR-VM16에 Netflow를 지원합니다
VM32용 Netflow	FC4-10-AIVMS-588-02-DD	FortiNDR-VM32에 Netflow를 지원합니다
FortiCare 및 업데이트	FC-10-AI3K5-331-02-DD	상시 FortiCare + FortiGuard 뉴럴 네트워크 엔진 업데이트 및 기준치.
FORTINDR 액세서리		
제품	**SKU**	**설명**
3.84TB 2.5" SATA SSD 트레이	SP-DFAI-3T	FortiNDR-3500F용 3.84TB 2.5" SATA SSD 트레이.
10GE SFP+ 트랜시버 모듈, 장거리	FN-TRAN-SFP+LR	10GE SFP+ 트랜시 모듈, 10km 장거리, SFP+ 및 SFP/SFP+ 슬롯이 있는 시스템.
10GE SFP+ 트랜시버 모듈, 단거리	FN-TRAN-SFP+SR	10GE SFP+ 트랜시버 모듈, 단거리, SFP+ 및 SFP/SFP+ 슬롯이 있는 시스템.
10GE 구리 SFP+ RJ45 트랜시버 (30m 거리)*5페이지 참조	FN-TRAN-SFP+GC	10GE 구리 SFP+ RJ45 트랜시버 모듈(30m 거리), SFP+ 슬롯이 있는 시스템
1GE SFP RJ45 트랜시버 모듈	FN-TRAN-GC	1GE SFP RJ45 트랜시버 모듈, SFP 및 SFP/SFP+ 슬롯이 있는 시스템.
FORTINDR CLOUD		
제품	**SKU**	**설명**
FortiNDRCloud-SAAS 서비스	FC1-10-NDRCL-667-02-12	측정 사용량 1Gbps에 대한 탐지, 조사, 플레이북, 보고서를 포함하는 FortiNDR Cloud 가이드형 SaaS 플랫폼에 대한 연간 구독 라이선스. FortiCare Primium이 포함됩니다. 물리적 센서는 포함하지 않습니다.
총 사용량	NDRC-TRUEUP-1MTH	1Gbps 측정 사용량에 대해 FortiNDR Cloud의 트래픽 초과분에 대한 처리량 합계 SKU.
FortiNDRCloud-500F	FNRC-500F	FortiNDR Cloud SaaS 플랫폼에 데이터를 전송하기 위한 FortiNDRCloud 500F (소형) 물리적 센서. 하드웨어만 포함됩니다. 1U 및 2 x 구리 / 2 x 섬유 SFP+. 지원을 구매해야 합니다. 2 x 10G 멀티모드 트랜시버와 함께 출고됩니다.
소형 센서 (500F) 라이선스 및 지원	FC-10-NDR5F-247-02-DD	FNRC-500F (소형) 센서 및 FortiNDR Cloud SaaS 플래숖ㅁ에 대한 포워딩 트래픽 지원을 위한 연간 라이선스, FortiCare Premium 포함.
FortiNDRCloud-900F	FNRC-900F	FortiNDR Cloud SaaS 플랫폼에 데이터를 전송하기 위한 FortiNDRCloud 900F (대형) 물리적 센서. 하드웨어만 포함됩니다. 1U 및 2 x 구리 / 2 x 섬유 SFP+. 지원을 구매해야 합니다. 4 x 10G 멀티모드 트랜시버와 함께 출고됩니다.
대형 센서 (900F) 라이선스 및 지원	FC-10-NDR9F-247-02-DD	FNRC-900F (대형) 센서 및 FortiNDR Cloud SaaS 플랫폼에 대한 포워딩 트래픽 지원을 위한 연간 라이선스, FortiCare Premium 포함.

Fortinet 기업의 사회적 책임 정책

Fortinet은 사이버 보안을 통해 모든 사람을 위한 발전과 지속가능성을 촉진하고, 인권과 윤리적 비즈니스 관행을 존중하고 항상 신뢰할 수 있는 디지털 세상을 실현하는 데 최선을 다하고 있습니다. 귀하는 Fortinet의 제품과 서비스를 사용하여 검열, 감시, 구금 또는 과도한 무력 사용을 포함한 인권 침해 또는 남용을 어떠한 방식으로도 관여하거나 지지하지 않을 것임을 Fortinet에 대변하고 보증합니다. Fortinet 제품 사용자는 Fortinet EULA를 준수하고 Fortinet 내부자고발 정책에 나와 있는 절차에 따라 EULA 위반이 의심되는 모든 사항을 신고해야 합니다.



www.fortinet.com/kr

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

2023년 5월 15일 월요일

FNDR-DAT-R11-20230515