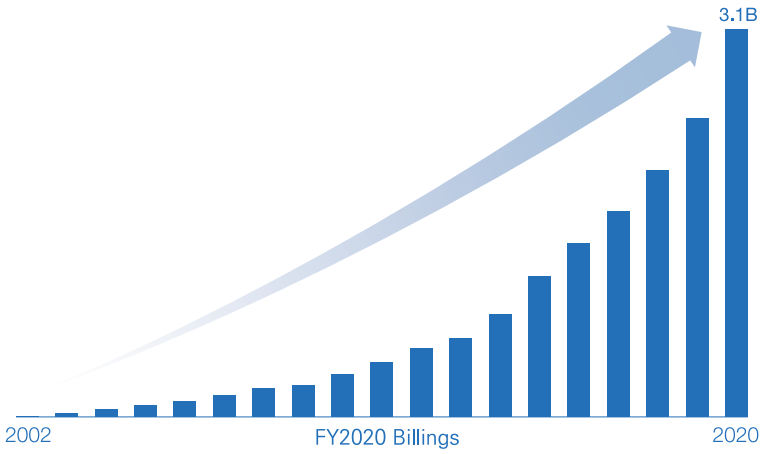
SECURITY. NETWORKING.

A LEADER.

Making possible a digital world
you can always trust

개요

Fortinet의 미션은 가장 혁신적인 최고 성능의 네트워크 보안 패브릭을 제공하여 IT 인프라의 단순화 및 안전화에 기여하는 것입니다. Fortinet은 네트워크 보안, SD-WAN, 스위칭 및 무선 액세스, 네트워크 액세스 제어, 인증, 퍼블릭 및 프라이빗 클라우드 보안, 엔드포인트 보안, AI 기반 지능형 보안 위협 보호 솔루션을 데이터 센터뿐만 아니라 엔터프라이즈 및 분산형 사무실에 제공하는 세계적 기업입니다.



디지털 혁신과 동반되는 위험 증가

규모와 관계없이 모든 조직은 경쟁력 향상, 운영 비용 절감, 새로운 제품 및 서비스 제공, 새로운 시장 진출 등 여러 가지 이유로 기술에 의존하고 있습니다. 하지만 바로 그러한 기술이 조직을 실제로 공격에 더 취약하게 만드는 예상치 못한 결과를 초래할 수 있습니다.

클라우드, IoT, SD-WAN과 같은 기술은 디지털 공격 표면을 넓히고, 보호하지 않은 채로 두면 사이버 범죄자에게 마치 열려 있는 문처럼 될 수도 있는 "엣지"를 네트워크에 만듭니다. 기업 네트워크에 들어가는 새로운 방법이 생겨남에 따라 점점 더 지능적인 위협이 개발되어 공격에 사용되고 있습니다.

기업들이 네트워크에서 보안 제품 수를 늘리는 방식으로 스스로를 보호하려고 함에 따라 운영은 점차 복잡해지고 있습니다. 여기에 더해 숙련된 인력까지 부족해서 문제가 더욱 심각해집니다. 따라서 디지털 혁신을 통해 얻으려고 했던 이점을 지연하거나 완전히 가로막는 최악의 상황이 발생할 수 있습니다.

설립: 2000년 11월
제품 첫 출시: 2002년 5월

Fortinet IPO: 2009년 11월
NASDAQ: FTNT

본사 위치: 캘리포니아주 서니베일
직원 수: 8,615명

올해 누적 출고 유닛: 680만 개 이상
고객 합계: 510,000명 이상
시가 총액: 33.8조원

포티넷 코리아
서울특별시 강남구 영동대로 325
S타워 14, 15층
대표전화: 080-559-8989
이메일: kr-callcenter@fortinet.com
홈페이지: www.fortinet.com/kr

포티넷 코리아 홈페이지

위협 인텔리전스의 힘

포티넷 보안 패브릭을 구성하는 다양한 기술 외에도 모든 것을 통합하는 또 하나의 중요한 요소가 있습니다. 바로 AI 중심 위협 인텔리전스입니다. 보안 인프라의 각 요소는 로컬 위협 인텔리전스의 소스 역할을 하면서 중앙 글로벌 인텔리전스 센터인 FortiGuard Labs에 실시간 정보를 다시 제공하는 것과 같은 이중 임무를 수행합니다. 이러한 정보를 신뢰할 수 있는 소스와 최고 수준의 위협 조사로부터 얻은 추가적인 위협 인텔리전스 스트림과 결합하여 FortiGuard Labs는 전 세계적으로 그리고 지속적으로 여러 로컬 시스템에 업데이트를 제공합니다.

주가 실적

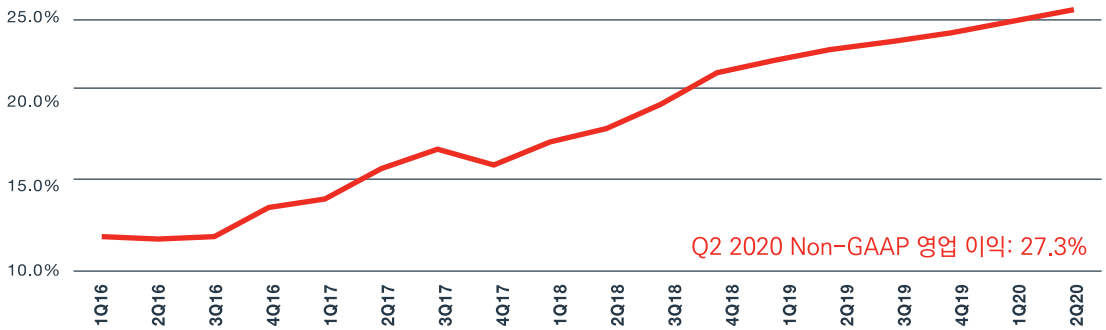
	1년	3년	5년	IPO 이후*
FTNT 순위	**1위**	**1위**	**1위**	**1위**
FTNT	**79%**	**267%**	**232%**	**2,096%**
CHKP	-7%	-2%	35%	224%
PANW	13%	72%	31%	447%

2020년 6월 30일까지 주가 실적. 출처: FactSet

* 2009년 11월 18일에 $6.25에 FTNT IPO(분할 조정됨), 2012년 7월 20일에 $42에 PANW IPO. FTNT IPO 날짜 이후 CHKP 실적.

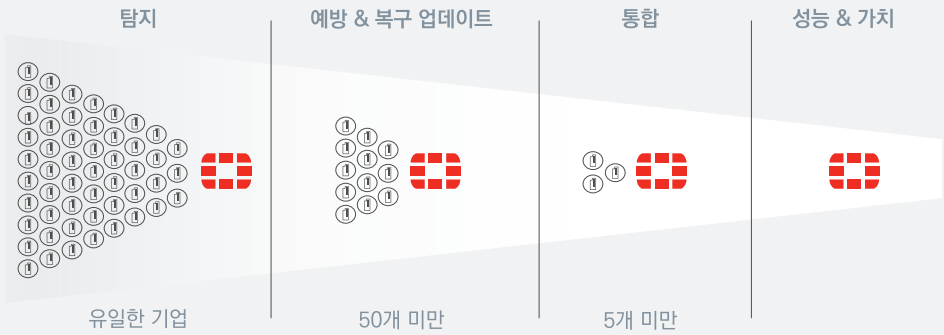
꾸준한 영업 이익 증가

Non-GAAP 영업 이익 – **4분기 연속 평균**



출처: 회사 데이터.

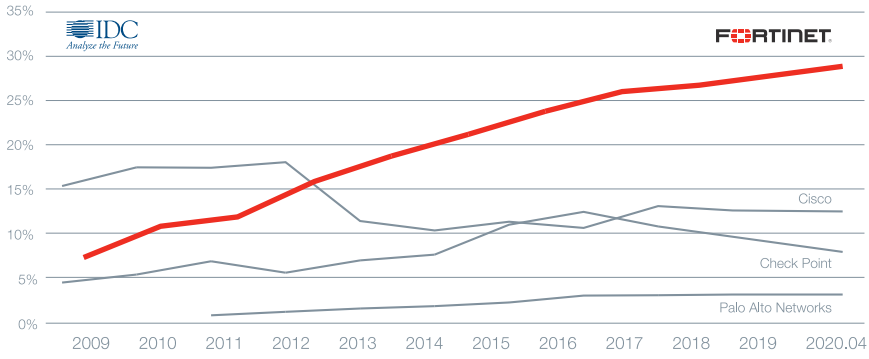
네트워크 보안의 모든 주요 단계에서 우수한 성능을 제공하는 유일한 기업



#1
가장 많이 배포된
네트워크 보안

전체 FW/UTM 장비 출고의 ~30%

출처: IDC Worldwide Security Appliance Tracker,
2020년 4월(방화벽, UTM, VPN 장비 연간 유닛 출하 기준)

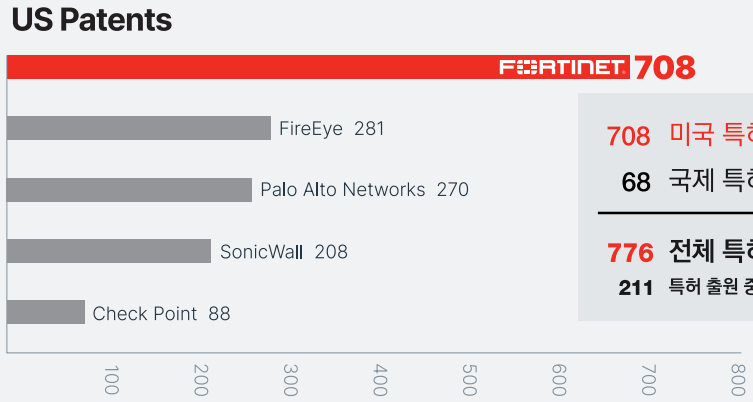


출처: IDC Worldwide Security Appliance Tracker, 2020년 4월(방화벽, UTM, VPN 장비 연간 유닛 출하 기준)

#1
네트워크 보안
혁신 기업

다른 네트워크 보안 기업보다
3배나 많은 특허 개수

지속적인 기술혁신을 위해
매출액의 약 20%를 R&D에 투자



708 미국 특허
68 국제 특허

776 전체 특허
211 특허 출원 중

출처: US Patent Office, 2021년 3월 31일 기준

#1
광범위한 보안 보호

IoT에서 클라우드까지 커버

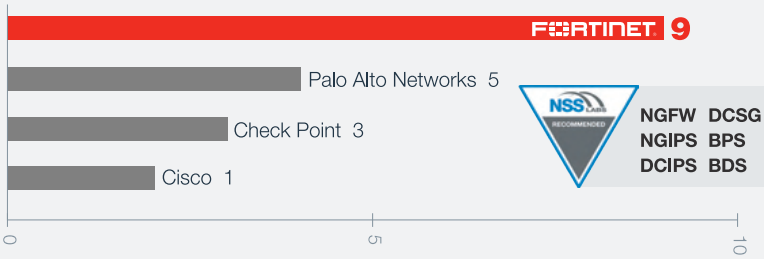
출처: 최근 분석가 조사에 따른 Fortinet 추정치.
2024년 기회.

총 진출 가능 시장 규모
$800억

2021 ~ 2024년까지
$1070억

#1
타사 검증
가장 우수한 평가

NSS Labs, ISCA, VB 등



NSS Labs RECOMMENDED

NGFW DCSG AEP
NGIPS BPS WAF
DCIPS BDS SD-WAN

Customer Briefing Center

포티넷 CBC를 방문하면 어떤 솔루션을 체험할 수 있나요?

전세계 TOP3 사이버 보안 벤더사이자, 국내 차세대 방화벽/UTM 시장 점유율 1위(외산 기준)를 차지한 포티넷이 국내 고객을 위한 보안 솔루션 체험 센터를 마련했습니다. 포티넷 CBC(Customer Briefing Center)에서는 포티넷이 제공하는 최고 성능의 방화벽과 혁신적인 제품 포트폴리오를 체험하실 수 있고, 각 고객의 방문 특성과 요구사항에 따라 맞춤화된 컨설팅으로 고객이 직면한 문제를 논의하고 해결할 수 있습니다.

차세대 방화벽 / UTM
보안 가시성 확보 및 통제,
암호 트래픽 내 악성코드를 탐지하는 솔루션

인공지능 ATP 솔루션
인공지능 AI 기반의 초고속 악성코드 탐지 및
ATP 샌드박스 기술

SIEM, SOAR
통합 이상행위 관제솔루션 SIEM, 보안정책
오케스트레이션 자동화 대응을 위한 SOAR

ATP 솔루션
사내 통신 또는 서버 팜에 업로드 되는 트래픽의
악성 파일 검출 솔루션

이메일 ATP 솔루션
이메일 보안 고도화 방안 및 URL과 첨부 파일의
악성코드 탐지 및 방어 기술

EPP, EDR, NAC
악성코드를 탐지하며 통제 시스템이 접속 허용 및
거부를 결정하는 솔루션

유 • 무선 네트워크 접속 통제 솔루션
접속 기기를 통제하기 위한 보안 스위치,
무선AP (WiFi 6) 컨트롤러 솔루션

CASB, CWP
멀티-클라우드 다이나믹 보안을 위한 차세대 방화벽과
CASB, CWP 솔루션

시큐어 웹 게이트웨이
내부 사용자의 유해 사이트 접속을 차단하는 솔루션

OT 보안 솔루션
OT 인프라 환경의 자산 정보 가시성을 확보하고
악성코드 탐지하는 솔루션

포티넷 CBC에 방문해야 하는 이유는 무엇일까요?

포티넷 CBC는 국내 최고의 보안 기업 포티넷의 브랜드, 비전, 다양한 혁신 제품, 보안 솔루션 및 서비스를 직접 체험하면서 특장점을 이해할 수 있도록 설계되었습니다. 이와 더불어 다음과 같은 고객의 현안을 포티넷의 솔루션으로 어떻게 해결할 수 있는지에 대한 방안을 제시합니다.

- **고객사의 디지털 트랜스포메이션에 필요한 IT 보안 요구 사항을 알아보고 최적의 해결 방안을 제시합니다 .**
- **고객의 비즈니스 목표에 맞추어 당사 기술 전문가와 1:1 맞춤 컨설팅이 가능합니다 .**
- **축적된 수많은 레퍼런스로 고객의 다양한 상황에 맞는 완벽한 보안 솔루션을 제공합니다 .**
- **보안 솔루션을 시각적으로 확인할 수 있는 라이브 데모를 직접 체험할 수 있습니다.**

Fortinet Next Generation Firewall / UTM Solution

포티넷 차세대 방화벽 / UTM 솔루션

보안 효율성

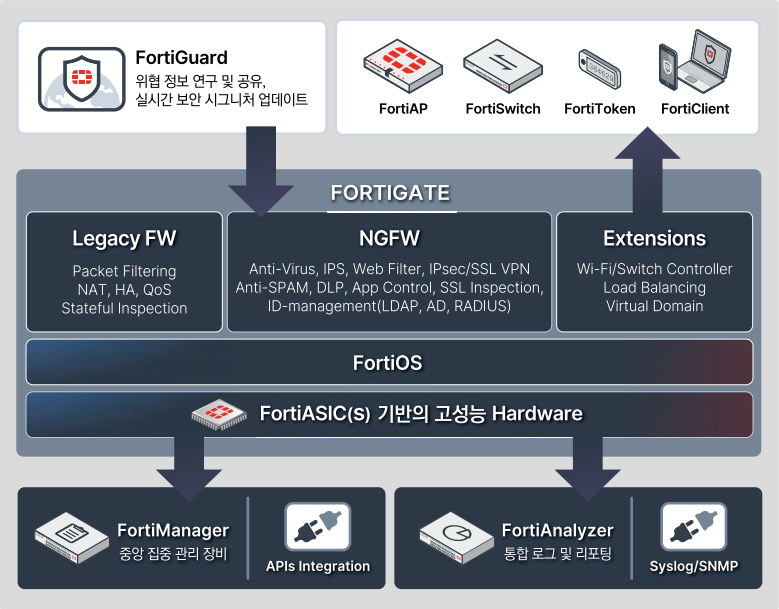
- 광범위한 위협에 대한 대응
- 빠른 보안 위협 시그니처 업데이트 제공
- APT 및 우회 공격을 방어
- 자체 가상화 기능 제공으로 물리적 공간 및 전력 효율성 확보

트래픽 가시성

- 응용 프로그램, 사용자, 장치 및 위협을 식별하여 보다 심층적인 정보를 제공
- 단일 화면을 통한 가시성과 풍부한 보고 기능을 제공

성능 및 신뢰성

- 자체 설계한 SPU(Security Process Unit) 활용
- 기능별로 사용자가 원하는 성능 유지
- 비즈니스 연속성 및 대역폭 요구 사항을 지원할 수 있는 성능
- 다양한 이중화 구성, 안정적인 Fail-over



차세대 방화벽 주요 모델별 사양

구분	FG-3300E (High-End)	FG-600E (Mid-Range)	FG-60F (Low-End)	FG-08VM (VMware ESXi 기준)
방화벽 성능 (1518/512/64 byte UDP)	160 / 158 / 100 Gbps	36 / 36 / 27 Gbps	10 / 10 / 6 Gbps	30.8 Gbps
Application Control 성능 (HTTP 64k)	70 Gbps	15 Gbps	1.8 Gbps	10.2 Gbps
IPS 성능 (Enterprise Mix)	27 Gbps	10 Gbps	1.4 Gbps	7.2 Gbps
NGFW 성능 (App control + IPS)	23 Gbps	9.5 Gbps	1 Gbps	5.9 Gbps
Threat Protection 성능 (NGFW + AV)	17 Gbps	7 Gbps	700 Mbps	4.5 Gbps
SSL Inspection 성능 (avg HTTPS)	21 Gbps	8 Gbps	630 Mbps	N/A
최대 동시 세션수 (CCS)	50 M	8 M	700 k	N/A (depend on MEM)
최대 초당 연결 수 (CPS)	700 k	450 k	35 k	150,000
최대 방화벽 정책	200,000	10,000	5,000	200,000
IPsec VPN 성능 (512byte)	98 Gbps	20 Gbps	6.5 Gbps	5.5 Gbps
최대 IPsec 터널 (GW to GW)	40,000	2,000	200	40,000
SSL VPN 성능	10 Gbps	7G bps	900 Mbps	4.5 Gbps
최대 SSL VPN user (터널모드)	30,000	10,000	200	10,000
Virtual Domain (default/max)	10 / 500	10 / 10	10 / 10	10 / 500
인터페이스	4x 40 GE QSFP+ 16x 25 GE/10 GE/1 GE SFP28 4x 10 GE RJ45 14x GE RJ45	2x 10 GE SFP+ 10x GE RJ45 8x GE SFP	10x GE RJ45	최대 24개

Fortinet ATP Solution

포티넷 ATP 솔루션

보안 패브릭을 통한 광범위한 공격 범위 커버

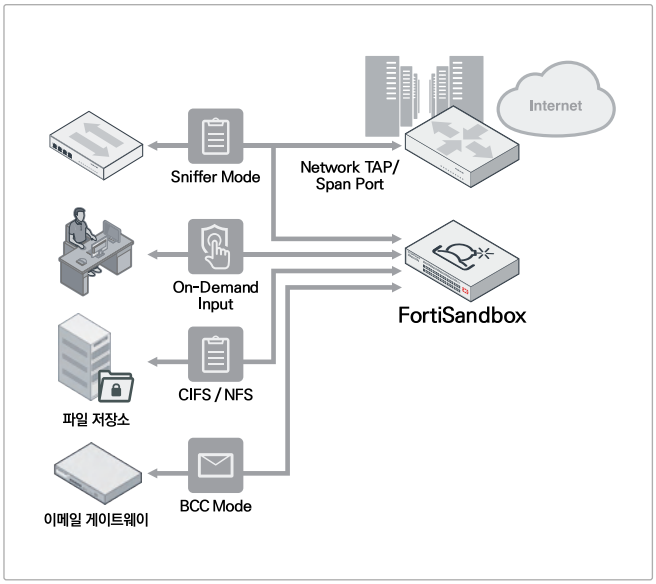
캠퍼스부터 퍼블릭 클라우드까지 네트워크, 이메일, 웹 어플리케이션, 엔드포인트를 보호하는 통합적이고 확장 가능한 아키텍쳐와 OT(Operational Technology)환경에서 발견되는 ICS(Industrial Control System) 장치를 통해 지능형 표적 공격을 효과적으로 방어합니다.

자동화된 제로데이, 지능형 멀웨어 탐지 및 대응

네이티브 통합 및 오픈 API가 포티넷과 타사 공급업체 보호 지점으로부터 객체를 전송하고, 즉각적인 위협 대응을 위해 실시간으로 위협 인텔리전스를 공유하고, 부족한 보안 리소스에 대한 의존도를 낮추는 과정을 자동화합니다.

인증 및 최고의 성능

NSS Labs, ICSA Labs와 같은 엄격한 현실의 독립 테스트를 지속적으로 거치고 있으며, 알려진 위협과 알려지지 않은 위협에 대처하는데 있어 지속적으로 최고 수준의 등급을 획득하고 있습니다.



FortiSandbox 주요 모델

FortiSandbox 500F | FortiSandbox 1000F | FortiSandbox 2000E | FortiSandbox 3000E

포티넷 ATP솔루션 주요 사양

구분	FSA-500F	FSA-1000F	FSA-2000E	FSA-3000E
폼팩터	1 RU	1 RU	2 RU	2 RU
총 네트워크 인터페이스	4x GE RJ45 포트	GE RJ45 포트 4개, GE SFP 슬롯 4개	GE RJ45 포트 4개, 10 GE SFP+ 슬롯 2개	GE RJ45 포트 4개, 10 GE SFP+ 슬롯 2개
스토리지	1x 1 TB	2x 1 TB	2x 2 TB	4x 2 TB
전원공급장치	1x PSU	1x PSU, 선택적 2x PSU	2x 예비 PSU	2x 예비 PSU
VM 개수	6	14	24	56
샌드박스 사전 필터 처리량(파일/시간)	4,500	7,500	12,000	15,000
VM 샌드박싱 처리량(파일/시간)	120	280	480	1,120
실제 유효 처리량(파일/시간)	600	1,400	2,400	5,600
스니퍼 처리량	500 Mbps	1 Gbps	4 Gbps	8 Gbps
높이 x 너비 x 길이(mm)	1.73 x 17.24 x 12.63	1.73 x 17.24 x 22.83	3.46 x 17.24 x 20.87	3.5 x 17.2 x 29
무게	18.72 lbs(8.5kg)	25 lbs(11.34kg)	27 lbs(12.25kg)	43 lbs(19.52kg)
전력 소비(평균/최대)	30.1/76.3 W	66.93/116.58 W	164.7/175.9 W	538.6/549.6 W
전원	100-240V AC, 50/60 Hz	100-240V AC, 50/60 Hz	100-240V AC, 50/60 Hz	100-240V AC, 50/60 Hz
작동 온도 범위	0-40 °C	0-40 °C	0-40 °C	10-35 °C
인증	FCC Part 15 Class A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST			

Fortinet CASB, CWP Solution

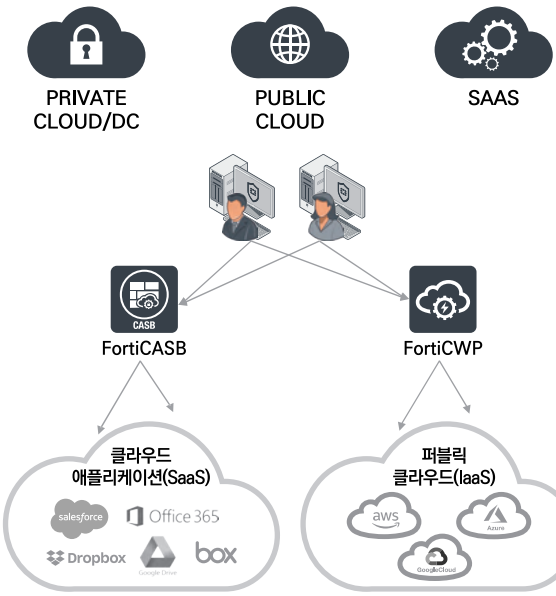
포티넷 CASB, CWP 솔루션

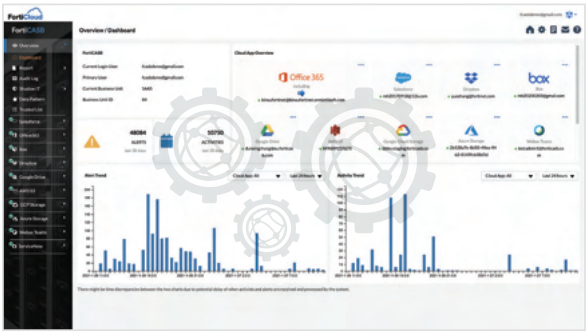
SaaS 애플리케이션에 대한 가시성 제공

- SaaS 애플리케이션을 사용 중인 기업의 주요 데이터를 모니터링하고, 민감한 정보 또는 기업의 중요 데이터가 유출되는 것을 방지합니다.
- 인가된 사용자와 비인가된 사용자를 구분하고, 인가되지 않은 사용자에게 기업의 민감한 정보가 공유되는 것을 추적 및 모니터링합니다.

퍼블릭 클라우드의 워크로드 모니터링 및 멀웨어 위협으로부터 기업의 주요 자산 보호

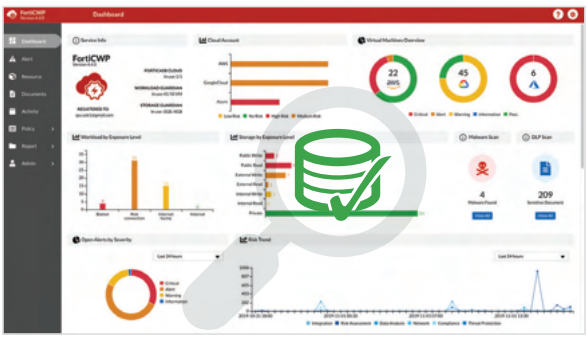
- 퍼블릭 클라우드에서 발생하는 사용자 워크로드 추적, 퍼블릭 스토리지에 저장되어 있는 소스코드 또는 파일에 기업의 위협요소가 있는지 추적 및 모니터링합니다.
- 포티넷의 검증된 시그니처 DB를 기반으로 퍼블릭 클라우드를 통해 공유될 수 있는 멀웨어 위협을 탐지하고 사전에 방지합니다.





FortiCASB

- 클라우드에 직접 액세스하여 조직의 데이터에 대한 가시성 제공
- 민감한 데이터 제어
- SaaS 애플리케이션을 통해 전파될 수 있는 위협을 탐지 및 추적



FortiCWP

- 클라우드 네이티브 '인프라를 대상으로 하는' Cloud Workload Protection 솔루션
- 클라우드의 위협 요소, 사용자 활동, 트래픽 Flow 및 스토리지 등, 구성 요소를 지속적으로 모니터링 및 추적
  - Botnet / CnC와 같은 악성 트래픽 모니터링
  - 의심스러운 사용자 활동 추적
  - 취약한 구성 검출
  - 민감한 데이터의 유출 및 저장된 데이터의 멀웨어 탐지

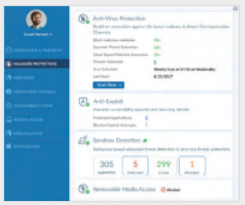
Fortinet EPP/EDR Solution

포티넷 EPP/EDR 솔루션

FortiClient / EMS

포티넷의 엔드포인트 보안솔루션인 FortiClient는 Anti-Virus엔진과 Anti-Exploit엔진을 이용하여 능동적인 엔드포인트 방어가 가능하며, VPN 기능을 제공하여 안전한 원격접속 기능을 제공합니다. 또한 패브릭 기반의 FortiClient는 EMS를 통해 통합된 엔드포인트 가시성 제공과 컴플라이언스 제어가 가능합니다.

패브릭 에이전트 | 취약점 관리 | 샌드박스 에이전트 | 원격접속 | 안티 바이러스 | 소프트웨어 인벤토리

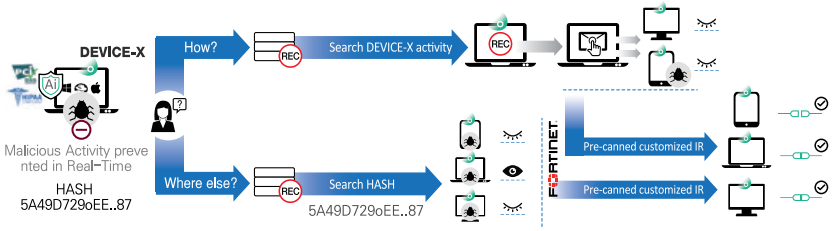


FortiClient 에이전트

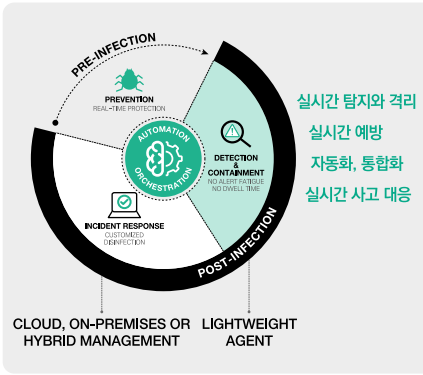
EMS(Enterprise Management System)

FortiEDR

FortiEDR은 자동화된 오케스트레이션을 포함하여 엔드포인트 침해탐지 및 대응과 함께 호스트 기반 차세대 안티바이러스 기능을 제공하는 포티넷의 엔드포인트 보안솔루션으로 글로벌 평가기관인 NSS Lab의 Advanced Endpoint Protection 추천등급으로 선정된 솔루션입니다.



FortiEDR을 통한 침해사고 분석



포티넷 EPP/EDR 솔루션 주요 사양

• FortiClient 운영체제별 지원 기능

주요기능	Windows	MAC OS X	ANDROID	iOS	CHROME BOOK	LINUX
엔드포인트 텔레메트리	✓	✓	✓	✓	✓	✓
액세스 제어를 통한 컴플라이언스 강화	✓	✓	✓	✓		✓
취약점 스캐닝을 통한 위협 완화	✓	✓				✓
엔드포인트 자동 격리	✓	✓				
안티 바이러스	✓	✓				✓
클라우드 기반 위협 탐지	✓					
안티 익스플로잇	✓					
샌드박스 연동 위협 탐지	✓	✓				✓
웹 필터링	✓	✓	✓	✓	✓	
어플리케이션 방화벽	✓	✓				
IPSec VPN	✓	✓	✓			
SSL VPN	✓	✓	✓	✓		✓
원격 로깅과 리포팅	✓	✓		✓	✓	✓
USB 디바이스 통제	✓	✓				✓

• FortiEDR 지원 운영체제

지원 OS	세부버전
Windows	XP SP2/SP3, 7, 8 and Win10
Win Server	2003 R2 SP2, 2008 SP2, 2008 R2, 2012, 2012 R2, 2016 and 2019
MacOS	Yosemite(10.10), EL Capitan(10.11), Sierra(10.12), High Sierra(10.13), Mojave(10.14) and Catalina(10.15)
Linux	Redhat Enterprise Linux, CentOS 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7 and Ubuntu LTS 16.04.5, 16.04.6, 18.04.1, 18.04.2 server
VDI	VMware Horizons 6 and 7, Citrix XenDesktop 7

• FortiEDR 리소스 사용량

리소스 종류	리소스 사용량
CPU	1% 미만 사용률
Memory	120 MB
Disk	20 MB

Fortinet Secure Web Gateway

포티넷 시큐어 웹 게이트웨이

웹 위협에 대한 지능형 보호

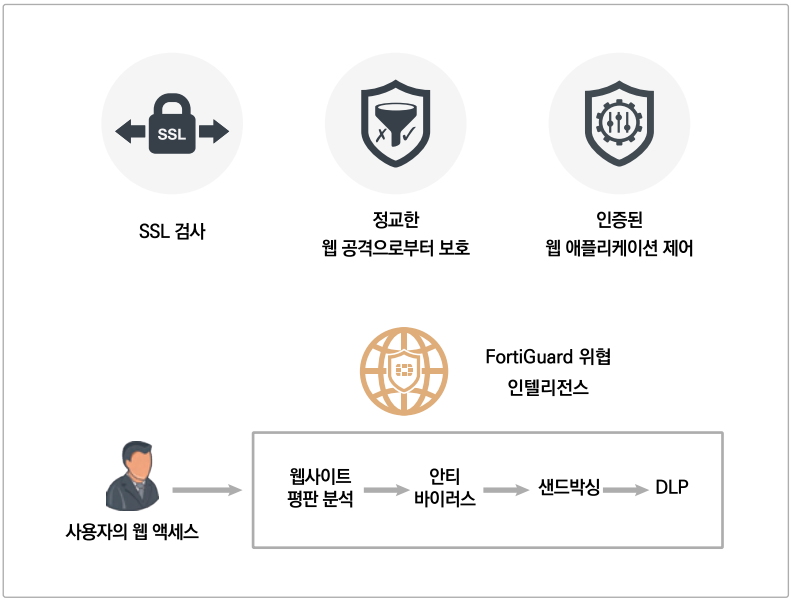
- FortiGuard 위협 인텔리전스 서비스와 통합
- 웹, DNS 필터링 및 애플리케이션 제어
- FortiSandbox 클라우드 및 온프레미스 어플라이언스와 통합
- AV, IPS, DLP 및 콘텐츠 분석

우수한 성능 및 확장성

- 우수한 성능을 제공하는 맞춤형 보안 처리 장치
- 뛰어난 확장성으로 소규모에서 대규모로 손쉽게 확장
- HA 구성을 통한 가용성 확보

콘텐츠 캐싱 및 WAN 최적화

- 정적, 동적 콘텐츠 캐싱
- 네트워크 지연 감소
- 낮은 대역폭 오버헤드



시큐어 웹 게이트웨이 라인업

	FPX400E	FPX2000E	FPX4000E
기본기능		Advanced Caching and WAN Optimization	
사용자 라이선스	500 ~ 4000 Users	2,500 ~ 25,000 Users	15,000 ~ 50,000 Users
인터페이스	4 x 10/100/1000 RJ45	2 x 10/100/1000 RJ45 2 x 10/100/1000 RJ45 bypass 2 x 1 GbE SFP 2 x 10 GbE SFP+	4 x 10/100/1000 RJ45 2 x 10/100/1000 RJ45 bypass 2 x 1 GbE SFP 4 x 10 GbE SFP+
Memory	8 GB	64 GB	128 GB
Storage	4TB (2 x 2 TB HDD)	8 TB (4 x 2 TB HDD) (plus 4 x 2 TB Optional)	8 TB (4 x 2 TB HDD) (plus 8 x 2 TB Optional)
SSL 하드웨어	2 x CP9	2 x CP9	2 x CP9
전원	단일 (이중화 옵션)	이중화	이중화

	FortiProxy VM01	FortiProxy VM02	FortiProxy VM04	FortiProxy VM08	FortiProxy VM16
하이퍼바이저 지원			VMware ESX / ESXi 플랫폼		
사용자 라이선스	100 Users	100 ~ 500 Users	100 ~ 2500 Users	100 ~ 10000 Users	100 ~ 25000 Users
하드웨어 사양	CPU 2, DISK 1개	CPU 4, DISK 2개	CPU 8, DISK 2개	CPU 16, DISK 4개	CPU 32, DISK 8개
네트워크 인터페이스	10	10	10	10	10

Fortinet AI ATP Solution

포티넷 인공지능 ATP 솔루션

가상 보안 분석가

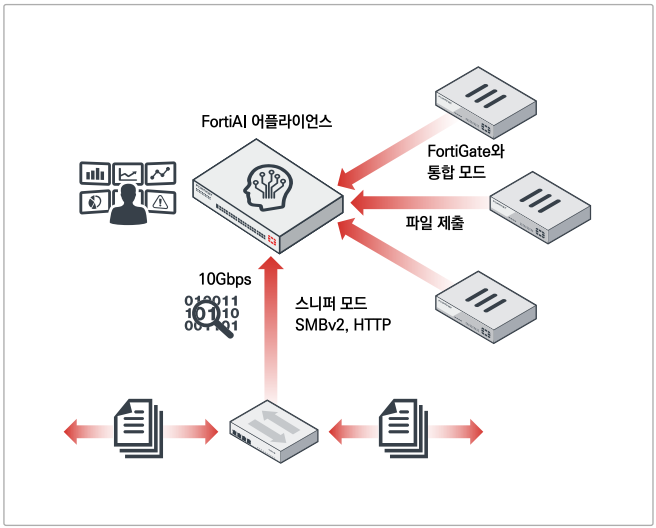
숙련 된 보안 분석가를 모방하기 위하여 인공지능 DNN(Deep Neural Networks)을 사용, 위협을 분류하여 보안 관제(SecOps)를 강화합니다.

위협 원천 차단

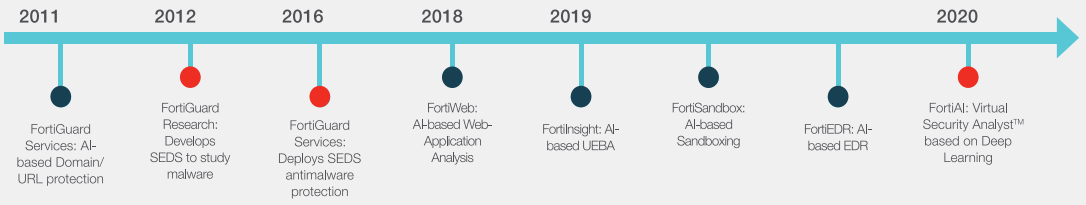
지속적으로 진화하는 학습 알고리즘을 기반으로 위협 특성을 과학적으로 분석하여 1초 이내에 정확한 판정을 생성함으로써 조직이 위협에 노출되는 시간을 크게 줄입니다.

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 · 시나리오 기반 엔진을 이용하여 최초 악성코드 근원지 탐지 · 유사성 엔진을 이용하여 네트워크에서 변종 악성 코드를 탐지 · MITRE ATT&CK 악성코드 매핑	· Pre-trained 되어 있는 수백만 개의 악성코드 DB · 아웃브레이크(Outbreak) 검색 엔진 (hash, virus family) · 파일 침해 지표 IOC (Indicator of Compromise) 분석	
디플로이먼트	· 스탠드 얼론 : 스니퍼 모드 · FortiGate와 연동 가능 · 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 – PE 파일 – DLLs – 실행 ZIP 파일
웹 / 텍스트 트래픽 – HTML, EXE, PDF, JS, VBS, VBA, DOC, PPT, XSLT, ELF, HWP (Hancom)
스니퍼 – HTTP, SMBv2, IMAP, POP, SMTP
FortiGate 연동 – HTTP, HTTPS (SSL 복호화), SMTP, POP3, IMAP, MAPI, FTP
수동 / REST API 업로드 – .tar, .gz, .tar.gz, .zip, .bz2, .rar

Fortinet LAN Edge Solution

포티넷 랜 엣지 솔루션 (유·무선 네트워크 통제 솔루션)

유무선 인프라 통합

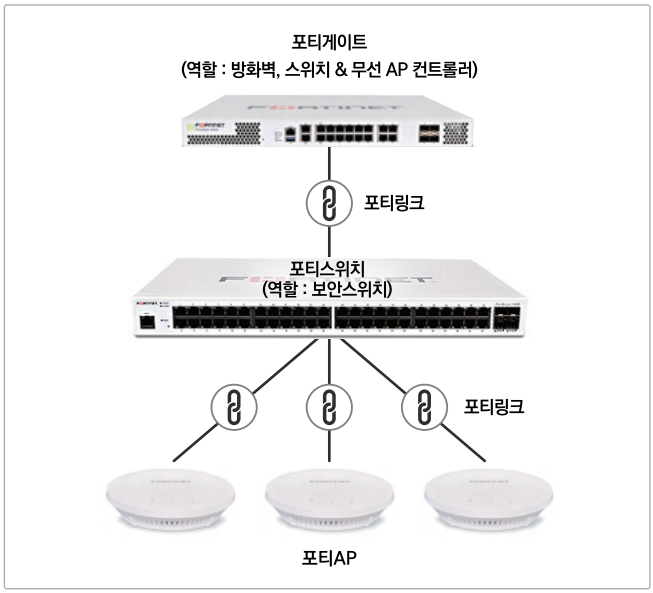
유선 LAN과 무선 Wi-Fi 인프라 통합 구축을 위한 네트워크 장비와 최신 보안 기술을 동시에 제공하여 네트워크 액세스 엣지 보안 및 다양한 고객환경에 적용되도록 설계된 통합 패키지를 제공합니다.

네트워크 엣지 보안

FortiOS를 통해 어떤 규모의 기업이라도 통합된 방화벽, IPS, 어플리케이션 제어 및 웹 필터링 등으로 최신 사이버 보안 위협에 대한 전방위적 방어뿐 아니라, 유무선 네트워크 관리 및 제어를 최적의 비용으로 운용이 가능합니다.

운영 및 관리 용이성

네트워크 토폴로지 기반의 가시성으로 높은 수준의 운영 환경을 제공하며, 단일 관리창을 통한 전체 네트워크 정보 습득 및 제어를 가능하게 해주고, 별도의 라이센스 등 추가비용 없이 손쉬운 유무선 네트워크 구축과 확장을 지원합니다.



매니지드 스위치 및 AP 기능 역할

	FORTISWITCH FORTILINK 모드 (FORTIGATE 적용)
관리 및 구성	
여러 스위치 자동 검색	예
FortiGate당 관리되는 스위치 개수	FortiGate 모델에 따라 8~300개 (관리자 가이드 참조)
FortiLink 스태킹 (자동 스위치 간 링크)	예
스위치 소프트웨어 업그레이드	예
중앙 집중형 VLAN 구성	예
스위치 POE 제어	예
링크 어그리게이션 구성	예
스패닝 트리	예
LLDP / MED	예
IGMP 스누핑	예 (1xxE-시리즈에서는 미지원)
L3 라우팅 및 서비스	예 (FortiGate)
정책 기반 라우팅	예 (FortiGate)
가상 도메인	예 (FortiGate)
보안 및 가시성	
802.1X 인증 (포트 기반, MAC 기반, MAB)	예
Syslog 컬렉션	예
DHCP 스누핑	예
기기 탐지	예
MAC 블랙 / 화이트리스트 등록	예 (FortiGate)
사용자 및 기기 정책 제어	예 (FortiGate)
UTM 기능	
방화벽	예 (FortiGate)
IPC, AV, 애플리케이션 제어, 봇넷	예 (FortiGate)
고가용성	
HA 클러스터에서 FortiLink, FortiGate 지원	예
FortiLink 연결에 대해 LAG 지원	예
FortiGate-FortiSwitch 간 Active-Active 분할 LAG로 고급 리던던시 확보	예 (FS-2xx, 4xx, 5xx)

802.11ax Wi-Fi6	주요 사양
FAP-U431F/433F	: Tri-Radio 5 GHz + 5 GHz + 2.4 GHz or 5 GHz + 2.4 GHz + scanning, 1x BLE : 4x4 MIMO, Up to 4,804 Mbps + 4,804 Mbps + 300 Mbps : Dual redundant PoE/PoE+(1x 10/100/1000/2500 Base-T RJ45, 1x 10/100/1000 Base-T RJ45), 1x Type A USB, 1x RS-232 RJ45 Serial : Up to 512 Clients per Radio1 and Radio2
FAP-431F/433F	: Tri-Radio 2.4 GHz + 5 GHz + scanning, 1x BLE : 4x4 MU-MIMO | Up to 1,147 Mbps + 2,402 Mbps : Dual redundant PoE/PoE+(1x 10/100/1000/2500 Base-T RJ45, 1 x 10/100/1000 Base-T RJ45), 1x Type A USB, 1x RS-232 RJ45 Serial : Up to 512 Clients per Radio1 and Radio2
FAP-U231F	: Tri Radio 5 GHz + 2.4 GHz + scanning or 5 GHz + 5 GHz + scanning 또는 5 GHz + 5 GHz + 2.4 GHz, 1x BLE/ZigBee : 2x2 MIMO | Up to 867 + 867 + 400 Mbps : 2x 10/100/1000 Base-T RJ45, 1x RS-232 RJ45 Serial : Up to 512 per Radio
FAP-231F	: Tri-Radio 5 GHz + 2.4 GHz + scanning, 1x BLE/ZigBee : 2x2 MU-MIMO | Up to 574 Mbps + 1,201 Mbps + scanning : 2x 10/100/1000 Base-T RJ45, 1x RS-232 RJ45 Serial : Up to 512 per Radio
FAP-23JF	: Tri-Radio 5 GHz + 2.4 GHz + scanning, 1x BLE/ZigBee : 2x2 MU-MIMO | Up to 574 Mbps + 1,200 Mbps + scanning : 7x 10/100/1000 Base-T RJ45 Ports (1x 802.3at PoE (PD), 1x 802.3af PoE (PSE), 2x Non-PoE Ports, 1x Pass-through in, 1x Pass-through out, 1x RS-232 RJ45 Serial : Up to 512 per Radio
OutDoor FAP-432F	: Tri-Radio 2.4 GHz + 5 GHz + scanning, 1x BLE/ZigBee : 4x4 MU-MIMO | Up to 1,147 Mbps + 2,402 Mbps : 1x 10/100/1000/2500 Base-T RJ45, 1 x 10/100/1000 Base-T RJ45 (802.3af PoE PSE), 1x RS-232 RJ45 Serial : Up to 512 per Radio
OutDoor FAP-234F	: Tri-Radio 5 GHz + 2.4 GHz + scanning | 2x 5 G antenna + 2x 2.4 G antenna + 1 dual , 1x BLE/ZigBee : 2x2 MU-MIMO | Up to 574 Mbps + 1,201 Mbps + scanning : 2x 10/100/1000 Base-T RJ45, 1x RS-232 RJ45 Serial : Up to 512 per Radio

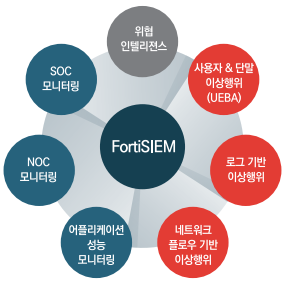
Fortinet SOC Solutions – FortiSIEM, FortiSOAR

포티넷 통합이상행위 관제 솔루션
지능형 SOC 업무 가속화 플랫폼

FortiSIEM – 통합이상행위 관제 솔루션

✓통합이상행위 관제 시스템

- SOC / NOC 통합
- 엔드포인트 / 네트워크 / 로그 모두 대응
- 시스템 자산 관리
- 위협 자동 대응
- 위협 인텔리전스 활용
- 머신러닝 기반 비정상 행위 탐지



✓Security Fabric 시너지

- SSL Inspection
- 광범위한 사이버공격 침입 경로 방어

✓Endpoint Agent 특징

- 가벼운 초소형 에이전트
- 호스트 수준 행위 로그 수집
  * File Activity – Create, Delete, read…
  * File Upload / Download
  * Drive(USB) mount / unmount
  * Log on / off…
  * UEBA 관점 이상행위 탐지

Model	FortiSIEM–500F "Collector"	FortiSIEM–2000F "Supervisor"	FortiSIEM–3500G "Supervisor"
AIO License Capacity	N/A	Up to 500	Up to 2,000
EPS Capacity	5,000 ingestion	Up to 5,000 ingestion	Up to 40,000 ingestion
Form Factor	1 RU	2 RU	4 RU
CPU	Intel Xeon E3-1225V3 4C4T 3.20 GHz	Intel Xeon E5-2620V3 6C12T 2.40 GHz	2 x Intel Xeon Gold 5118 12C24T 2.30 GHz
Total Interfaces	4 x 1 GbE (RJ45)	4 x 1 GbE (RJ45)	2 x GbE RJ45 ports, 2 x GbE SFP ports, 2 x 25 GbE SFP28
Storage Capacity	3 TB (1 x 3 TB) Max. 4 x HDD	36 TB (12 x 3 TB) Max. 12 x HDD	96 TB (4 TB x 24) Max. 24 x HDD
Memory	DDR3 16 GB (2 x 8 GB)	DDR4 32 GB	DDR4 128 GB (16 GB x 8 ECC REG Memory)
Rack Units	1	2	4
AC Power Supply	1	2	2

FortiSOAR – 지능형 SOC 업무 가속화 플랫폼

Specification	Recommended	Minimum
CPU	8	8
Memory	32 GB	22 GB
Disk	1 TB (SSD)	500 GB (SSD)
NIC	1EA	1EA
비고	※ 설치 환경에 따른 권장사양 협의	

엔드포인트에서 클라우드까지 단일 플랫폼 가시성 확보

✓SOC 업무 프로세스 통합

- 경고 / 인시던트 / 업무 프로세스 통합
- 보안팀 대응능력 상향평준화
- 이기종 다양한 운영 시스템 중앙 제어
- ROI / MTTD / MTTR 향상
- 사용자 에러 방지(Human Error)
- 사용자를 위한 강력한 커스터마이징 (UI&Report)

✓오케스트레이션 & 자동화(Playbook)

- 업무 프로세스 자동화
- 병렬 처리 / 큐 처리로 빠른 보안 위협대응
- 300+개 연동모듈
- 3,000+개 사용가능 플레이북 액션
- 단순 반복 작업 자동화
- SOC 사이버 피로도 감소
- 1,000+개 제조사 플레이북

자동화 기반 보안업무 플랫폼을 통해 SOC 업무 가속화

Fortinet Email ATP Solution

포티넷 이메일 ATP솔루션

위협 예방

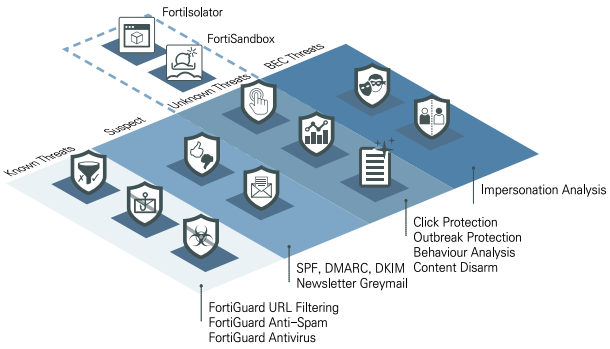
FortiMail은 강력한 스팸 방지 및 악성코드 방지 엔진을 통해 악성코드 감염을 방지하고, 콘텐츠 무장 해제 및 재구성, 샌드박스 연동을 통한 행위 분석, 명의 도용 탐지 및 원치 않는 대량 이메일, 피싱, 랜섬웨어를 차단하는 다양한 고급 기술들을 통해 이메일로 유입되는 다양한 위협들을 방어할 수 있습니다.

데이터 보호

강력한 데이터 손실 방지, ID 기반 이메일 암호화 및 보관은 기업의 민감한 정보의 부주의한 손실을 방지하고 산업 규정을 준수하는 데 도움이 됩니다.

시큐리티 패브릭 연동

FortiMail은 보안 패브릭을 통해 Fortinet 제품 및 타사 구성 요소와의 통합으로 IoC를 공유하여 보안에 대한 사전 예방적 접근 방식을 채택할 수 있습니다. 또한 API 수준의 통합을 통해 Microsoft 365 환경에 대한 고급 이메일 보호를 가능하게 합니다.



· FortiMail 주요 모델

FortiMail 200F　FortiMail 400F　FortiMail 3200E

· FortiMail 주요 탐지 평가 결과

99.9%
멀웨어 유형 및 멀웨어 제품군 전반에 걸친 악성 이메일 탐지.

94%
탐지율

99.71%
스팸차단률

99.5%+
악성코드 탐지율

포티넷 이메일 ATP 솔루션 스펙정보

구분	FortiMail-200F	FortiMail-400F	FortiMail-900F	FortiMail-3200E
보호 이메일 도메인	20	100	800	2,000
수신자 기반 정책(도메인별/시스템별)	60 / 300	400 / 1,500	800 / 3,000	1,500 / 7,500
서버모드 메일박스	150	400	1,500	3,000
안티스팸, 안티바이러스, 콘텐츠 프로파일 수(도메인별/시스템별)	50 / 60	50 / 200	50 /400	50 / 600
데이터 유출 방지	미지원	지원	지원	지원
Microsoft 365 API 연동	미지원	옵션	옵션	옵션
이메일 라우팅(시간당)	50,000	250,000	800,000	3,400,000
포티가드 엔터프라이즈 ATP(시간당)	30,000	150,000	400,000	2,000,000
파워 서플라이	Single	Single (Dual Optional)	Dual	Dual
폼 팩터	랙마운트, 1 U	랙마운트, 1 U	랙마운트, 1 U	랙마운트, 2 U
스토리지	1 x 1 TB	2x 1 TB	2x 2 TB	2x 2 TB
네트워크 인터페이스	4x 10/100/1000 (Copper, RJ45)	4x 10/100/1000 (Copper, RJ45)	4x 10/100/1000 (Copper, RJ45), 2x SFP GE	4x 10/100/1000(Copper, RJ45), 2x SFP GE, 2x SFP+ 10 GE
컴플라이언스	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, RoHS			
인증	VBSpam & VB100 rated, Common Criteria NDPP, FIPS 140-2 Compliant			

Fortinet ICS/OT Solution

포티넷 ICS/OT 솔루션

견고한 디자인

팬이없고 견고한 구성품을 사용하여 열악한 산업 환경에서 안정적인 작동을 보장합니다.

통합 보안 아키텍처

FortiOS 통합 보안을 실행하는 FortiGate는 다중 포인트 제품보다 더 나은 보호와 낮은 소유 비용을 제공합니다. FortiGuard 산업 보안 서비스와 결합하여 중요한 네트워크가 실시간 보호를 받도록 합니다.

관리 용이성

신속한 프로비저닝 및 배포, 장치 및 위협 상태 모니터링을 허용하는 강력한 관리 시스템으로 실행 가능한 보고서를 제공합니다.

FortiGate, FortiSwitch, FortiAP Rugged Series

FSR-112D-POE and FSR-124D

FortiAP 222C

IEC 61850-3 IEEE 1613 | ICSA labs CERTIFIED | FIPS 140-2 | COMMON CRITERIA CERTIFIED EAL4+

FGR-30D
- IP20, Indoor Use
- Dual-input power
- Industry Certified

FGR-35D
- IP67, Outdoor Use
- Industry Certified

FGR-60F
- IP20, Indoor Use
- SoC4 Powered
- By-pass port
- Industry Certified

FGR-90D
- IP40, Indoor Use
- By-pass port
- Dual-input power
- Industry Certified

방화벽 및 관리 솔루션 모델별 기능 역할

구분	FortiGate-1101E	FortiGate-101F	FortiGate Rugged 60F	FortiManager 300F	FortiAnalyzer 800F
역할	IT & OT 경계 구간(Level 3.5)	OT망 (Level 1~2)	실외 구간	방화벽 중앙관리	통합로깅 시스템
방화벽 성능 (UDP 64 byte)	45 Gbps	10 Gbps	6 Gbps	N/A	N/A
Application ctl. 성능 ((HTTP 64K)	26 Gbps	2.2 Gbps	1.8 Gbps	N/A	N/A
IPS 성능	12.5 Gbps	2.6 Gbps	1.4 Gbps	N/A	N/A
방화벽 + IPS + Application 컨트롤 성능	9.8 Gbps	1.6 Gbps	1 Gbps	N/A	N/A
방화벽 + IPS + Application컨트롤 + Anti-Virus 성능	7.1 Gbps	1 Gbps	700 Mbps	N/A	N/A
최대 세션 수(CCS)	8 백만	1.5 백만	70 만	N/A	N/A
초당 세션 수(CPS)	50 만	56,000	35,000	N/A	N/A
레이턴시(지연율)	2.76 μs	4.97μs	3.3 μs	N/A	N/A
최대 연결 FortiSwitch/FortiAP	196 / 4,096	24 / 64	16 / 64	N/A	N/A
디스크	960 GB	480 GB	N/A	16 TB (4 x 4 TB)	16 TB (4 x 4 TB)
방수/방진/방습	N/A	N/A	지원	N/A	N/A
방화벽 통합 관리(정책, 오브젝트 등)	N/A	N/A	N/A	100대 관리	N/A
로깅 기능	○	○	○	N/A	○
인터페이스	2x 40 GE QSFP+, 4x 25 GE SFP28/10 GE SFP+, 4x 10 GE SFP+, 8x GE SFP, 18x GE RJ45	2x 10 GE SFP+, 18x GE RJ45, 4x Shared Port Pairs, 8x GE SFP	10x GE RJ45	4 x GE RJ45, 2 x SFP	4 x GE RJ45, 2 x SFP

Fortinet Secure SD-WAN

포티넷 시큐어 SD-WAN 솔루션

사용자 경험 향상

애플리케이션의 정확한 식별, WAN 성능 모니터링, 가속화된 클라우드 온램프를 통해 최적화된 네트워크 및 애플리케이션 성능을 제공합니다.

효율적인 운영

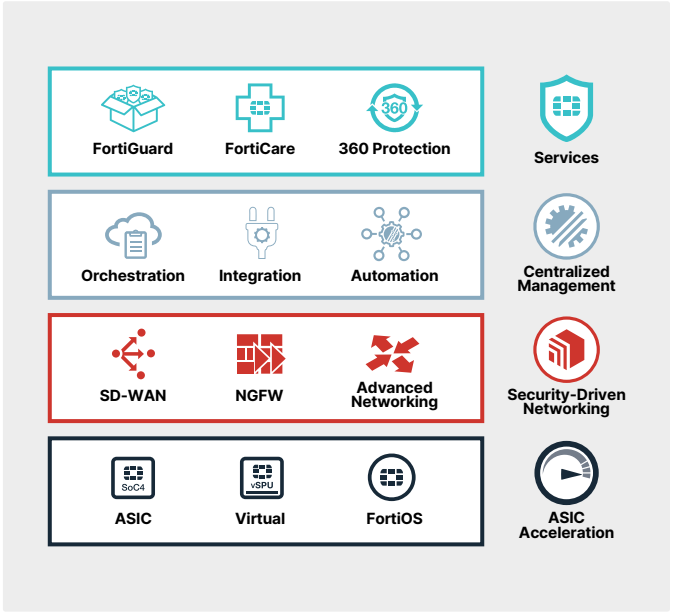
대규모 SD-WAN, 보안 및 SD-Branch에 대한 중앙 집중식 오케스트레이션 및 향상된 분석으로 운영을 간소화합니다.

통합 기능 가속화

업계에서 유일하게 특수 제작된 ASIC 기반 SD-WAN은 씬 엣지(SD-WAN, 라우팅) 및 WAN 엣지(SD-WAN, 라우팅, NGFW)를 지원하여 장소에 관계없이 모든 애플리케이션, 사용자 및 데이터를 보호합니다.

보안 및 가용성 확보

SD-WAN에 내장된 NGFW(차세대 방화벽)는 SD-WAN과 보안 기능을 통합 솔루션으로 결합하여 네트워크의 보안과 가용성을 유지합니다.



Secure SD-WAN 지점 장비 모델별 사양

구분	SMALL RETAIL/ HOME OFFICE	BRANCH/ SMB	BIG RETAIL/ SMB	MEDIUM BRANCH	LARGE BRANCH/ CAMPUS
권장 사용자 수	10	20	50	250	500
모델명	**FG-40F**	**FG-60F**	**5FG-80F**	**FG-100F**	**FG-200F**
IPsec VPN 성능	4.4 Gbps	6.5 Gbps	7.5 Gbps	11.5 Gbps	13 Gbps
최대 IPsec 터널	200	200	200	2500	2500
Threat Protection 성능	600 Mbps	700 Mbps	900 Mbps	1 Gbps	3 Gbps
App Control 성능	990 Mbps	1.8 Gbps	1.8 Gbps	2.2 Gbps	13 Gbps
SSL Inspection 성능	310 Mbps	630 Mbps	715 Mbps	1 Gbps	4 Gbps
최대 대역폭 제한	제한 없음	제한 없음	제한 없음	제한 없음	제한 없음
Zero Trust Network Access(ZTNA)	지원	지원	지원	지원	지원
인터페이스	5 x GE RJ45	10 x GE RJ45	8 x GE RJ45 2 x Shared Port Pairs	18 x GE RJ45 8 x GE SFP 2 x 10 GE SFP+ 4 x Shared Port Pairs	18 x GE RJ45 8 x GE SFP 4 x 10 GE SFP+
모델 선택 옵션	WiFi, 3G4G	WiFi, Storage	WiFi, Bypass, POE, Storage	Storage	Storage
확장성	FortiAP, FortiSwitch, FortiExtender 연동 지원				
폼 팩터	Desktop	Desktop	Desktop	1RU	1RU
전원 이중화	미지원	미지원	지원(옵션)	지원	지원

Fortinet Zero Trust Network Access

포티넷 ZTNA 솔루션

FortiClient Zero Trust Network Access

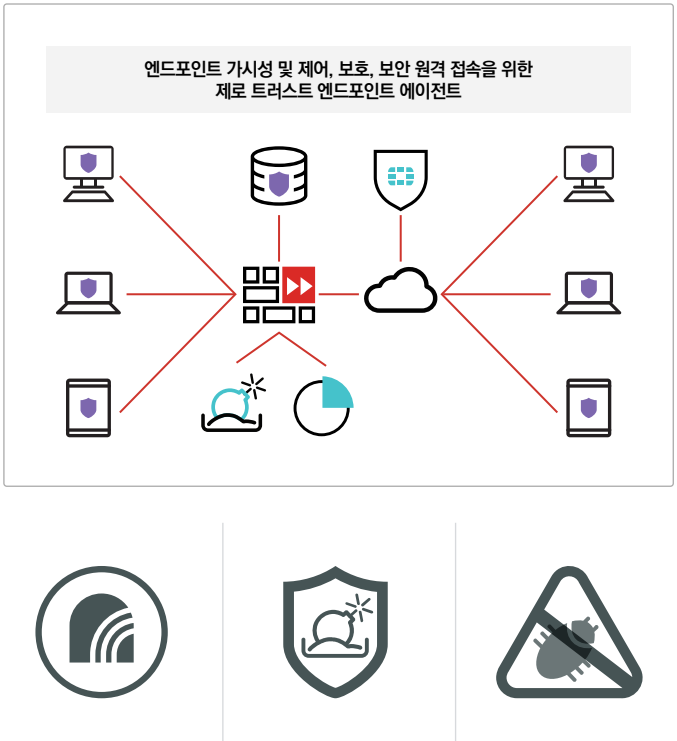
FortiClient ZTNA는 FortiOS와 함께 작동하여 사용자가 로컬 또는 원격에 관계없이 애플리케이션에 대한 세분화된 보안 액세스를 지원합니다. 각 세션은 사용자 및 사용자 단말기 확인을 위해 FortiClient에서 FortiOS 프록시 포인트로 자동 암호화된 터널로 시작됩니다. 사용자 및 사용자 단말기가 확인되면 해당 세션에 대한 액세스 권한이 부여됩니다. 또한 멀티액터 인증을 사용하여 추가 보안 계층을 제공할 수 있습니다. ZTNA를 사용하는 조직은 더 나은 원격 액세스 솔루션과 엔드포인트 위치에 관계없이 애플리케이션에 대한 액세스를 제어할 수 있는 일관된 정책을 모두 활용할 수 있습니다.

멀웨어 및 취약점 악용 차단

FortiClient는 FortiClient Cloud Sandbox와 통합하고 FortiGuard 글로벌 위협 인텔리전스를 활용하여 엔드포인트에 다운로드 되는 모든 파일을 분석하고, 알려지거나 알려지지 않은 멀웨어에 대한 정보를 공유하며 지능형 악성코드 및 취약점이 악용되는 것을 차단합니다.

엔드포인트 무결성

FortiClient는 회사 단말의 취약성 스캐닝 및 선택적 자동 패치를 통해 공격 표면을 줄이는 데 도움이 됩니다. 제로 트러스트 액세스 원칙과 결합된 이 접근 방식은 회사의 무결성 및 보안 태세를 강화할 수 있습니다.



포티넷 Zero Trust Network Access 솔루션 기능 정보

• FortiClient Zero Trust Security

주요기능	Windows	MAC OS X	ANDROID	iOS	CHROME BOOK	LINUX
엔드포인트 텔레메트리	✓	✓	✓	✓	✓	✓
액세스 제어를 통한 컴플라이언스 강화	✓	✓	✓	✓		✓
취약점 스캐닝을 통한 위협 완화	✓	✓				✓
IPSec VPN	✓	✓	✓			
SSL VPN	✓	✓	✓	✓		✓
원격 로깅과 리포팅	✓	✓		✓	✓	✓
USB 디바이스 통제	✓	✓				✓
Windows AD SSO Agent	✓	✓				
ZTNA Remote Access	✓	✓				✓

• FortiClient Endpoint Security

주요기능	Windows	MAC OS X	ANDROID	iOS	CHROME BOOK	LINUX
안티바이러스	✓	✓				✓
클라우드 기반 위협 탐지	✓	✓				
샌드박스 연동 위협 탐지 (on-premise)	✓	✓				✓
샌드박스 연동 위협 탐지 (클라우드 기반)	✓	✓				
엔드포인트 자동 격리	✓	✓				
웹필터	✓	✓	✓	✓	✓	
안티 익스플로잇	✓					
어플리케이션 방화벽	✓	✓				

포티넷 코리아 **주소** 서울특별시 강남구 영동대로 325 S-TOWER 14/15층
전화 080-559-8989 **이메일** kr-callcenter@fortinet.com **페이스북** http://www.facebook.com/FortinetSouthKorea
www.fortinet.com/kr