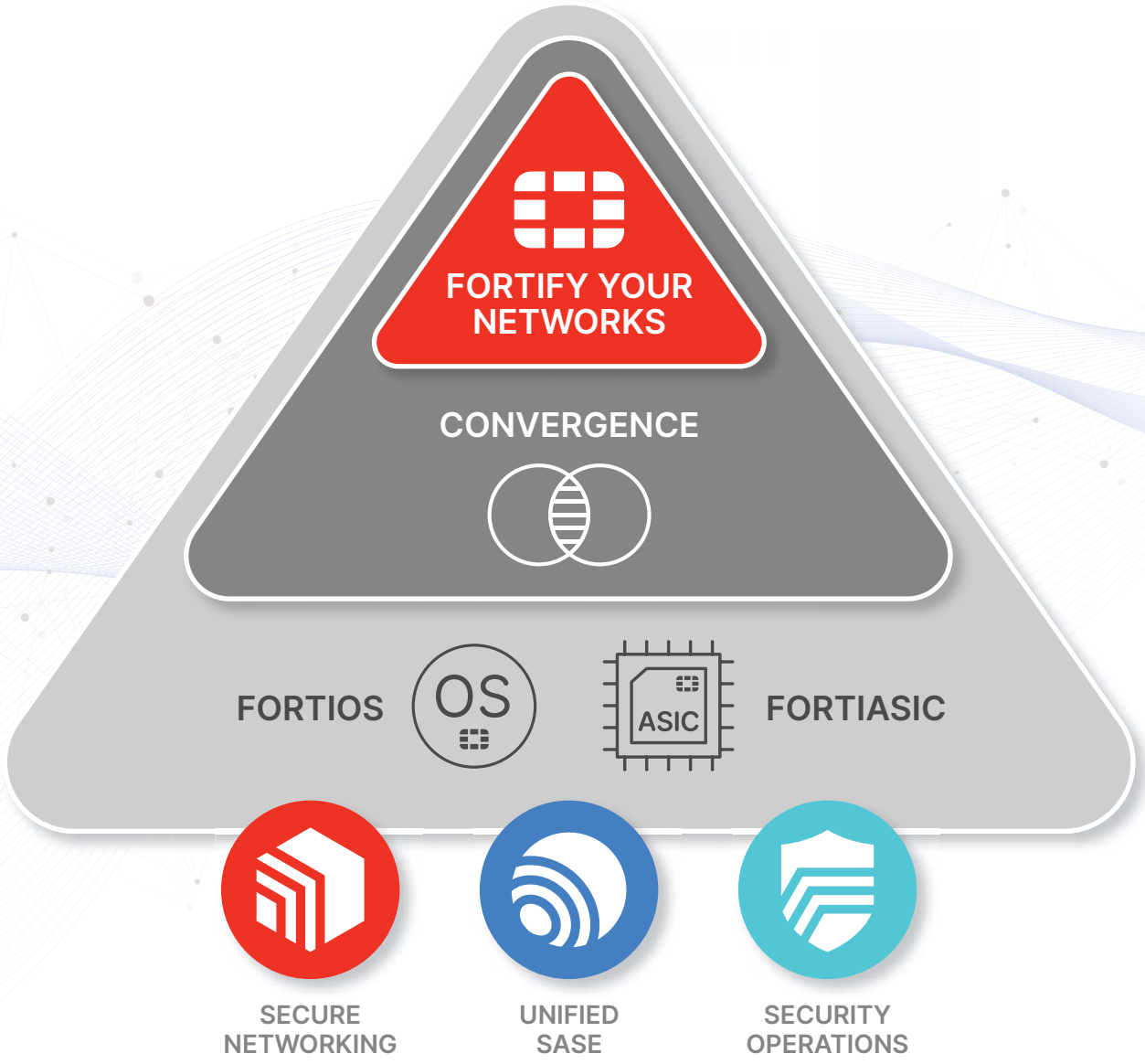
INTRODUCE

포티넷 회사소개서



목차

FORTINET

FY 2023 실적

매출
7조 3천억원

거래액
8조 8천억원

2023 4분기 실적

매출
1조 9천억원

거래액
2조 6천억원

운영마진
(GAAP) 27.2%

EPS(GAAP)
$0.40/주

현금 + 투자
3조 3천억원

시가총액
62조원
(AS OF DEC. 31, 2023)

고객수

755,000+

누적 출고량

1억 1,8000만대 이상

지역별 인원

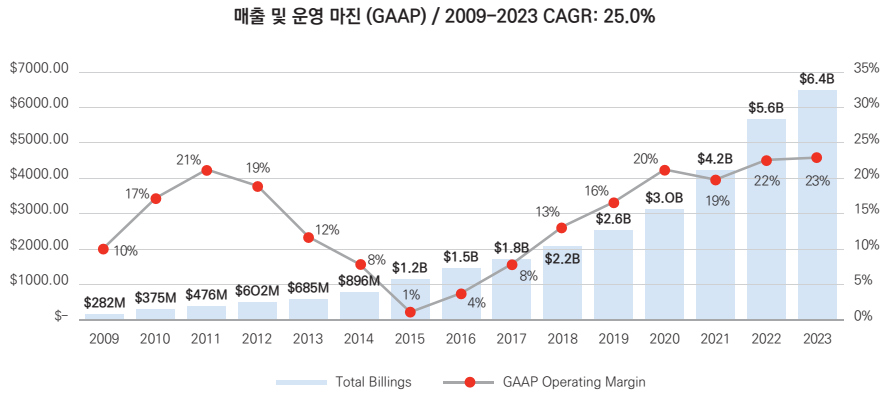
AMERICAS	미국	3,826
	캐나다	2,594
	나머지 미주 지역	987
EMEA	프랑스	519
	영국	451
	나머지 유럽, 중동 및 아프리카 지역	2,456
APAC	인도	722
	일본	627
	나머지 아시아 태평양 지역	1,386
총합		13,568

2023년 12월 31일 기준

Securing People, Devices, and Data Everywhere

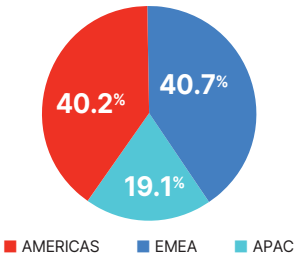
- **설립 연도 :** 2000년 8월
- **본사 위치 :** 미국 캘리포니아 주
- **IPO 시기 :** 2009년 11월
- **다우존스 지속가능경영지수(DJSI)에 편입**
- **나스닥 100 및 S&P 500 지수 편입**

연간 매출 및 수익성을 통한 글로벌 리더

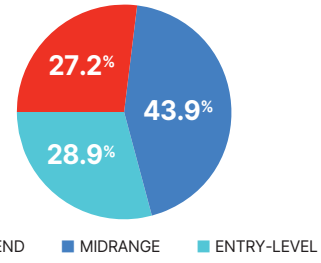


지역 및 세그먼트에 따른 다각화

2023년 4분기
지역별 매출

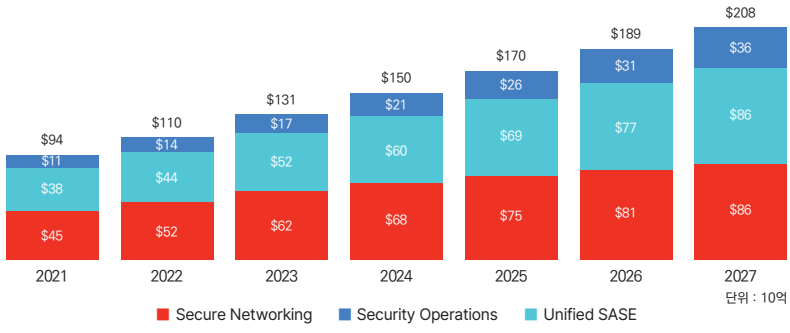


2023년 4분기
세그먼트별 거래액



성장하고 있는 거대한 보안 시장

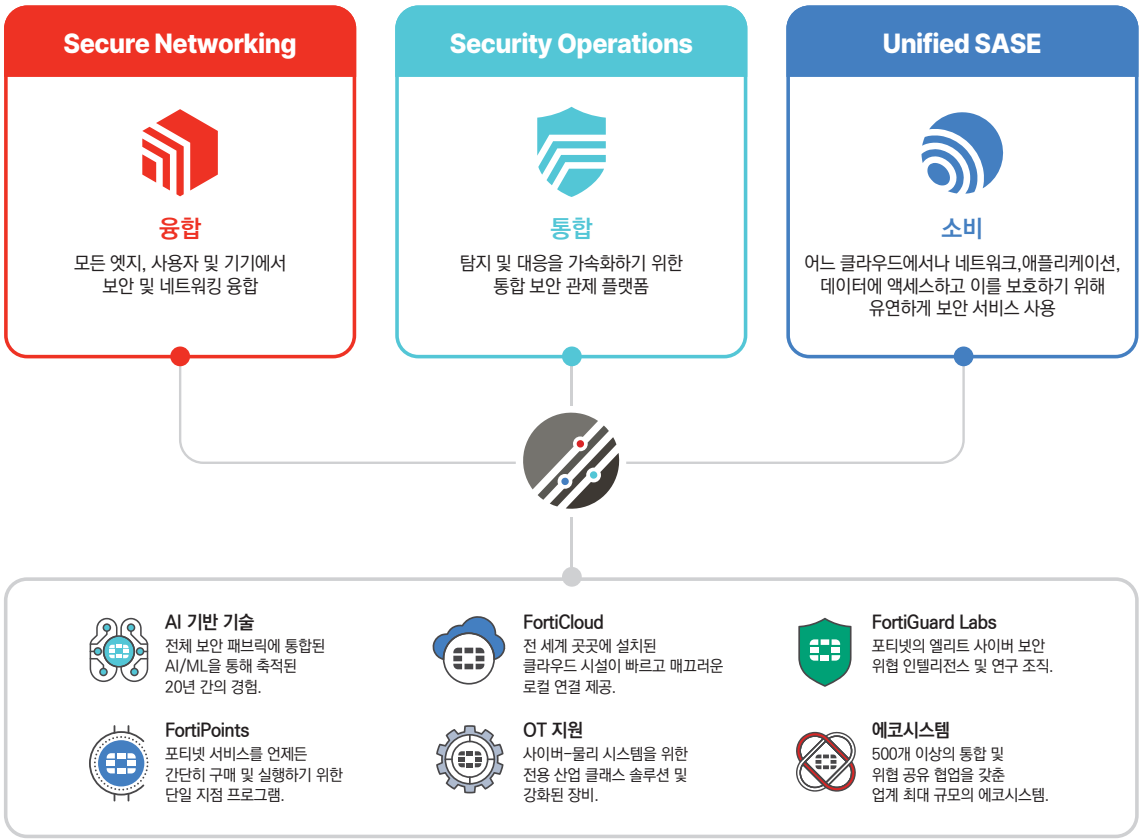
2027년까지 287조원 까지 성장 예정



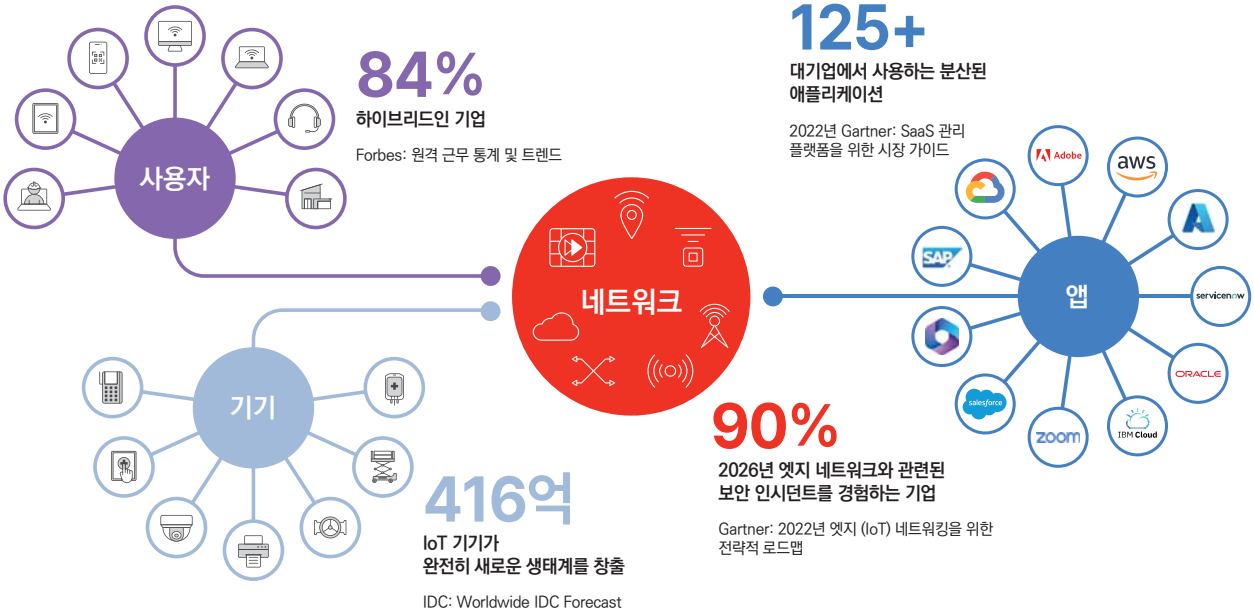
출처: 최근 분석 조사에 따른 포티넷 추정

포티넷 시큐리티 패브릭: AI 기반 플랫폼 전략

포티넷 통합 플랫폼 내에서 사이버 보안을 재정의하는 세 가지 솔루션이 끊임없이 진화하는 사이버 보안 환경에 대응하여 끊임없이 가속화되는 비즈니스 요구 사항을 충족할 수 있도록 지원합니다. 복잡한 네트워크, 분산된 사용자, 하이브리드 애플리케이션을 간소화하기 위한 방법은 보안을 융합 및 통합하고 유연한 소비 모델을 통해 쉽게 구매할 수 있도록 하는 것입니다.



복잡해진 인프라로 인해 가중된 공격 취약성



FORTINET

CBC 고객 솔루션 체험 센터

전 세계 TOP 사이버 보안 벤더인 포티넷에서
국내 고객분들을 위해 마련한 솔루션 체험 센터로
방문하시는 고객분들의 요구사항에 따라
맞춤화된 컨설팅을 제공합니다.

포티넷 CBC에 방문해야 하는 이유?

- 디지털 트랜스포메이션에 필요한 IT보안 요구사항을 알아보고 최적의 해결 방안을 제시합니다.
- 고객의 비즈니스 목표에 맞추어 당사 기술 전문가와 1:1 맞춤 컨설팅이 가능합니다.
- 보안 솔루션을 시각적으로 확인할 수 있는 라이브 데모를 직접 체험할 수 있습니다.
- 아시아 최대 규모의 보안 솔루션 체험 센터로, 어떤 상황에서도 완벽한 솔루션을 제공합니다.
- CBC 규모 증설로 추가적인 체험 신청을 받고 있습니다. 예약을 원하시는 고객분께서는 방문 예약 부탁드리겠습니다.

Secure Networking | **Security Operations** | **Unified SASE**

CBC 방문 신청하기

Virtual CBC 바로가기

포티넷 CBC는 언제나 여러분께 열려있습니다. 지금 방문 신청해주세요!

www.fortinet.com/kr/corporate/cbc

포티넷 차세대 방화벽

포티게이트 NGFW는 맞춤형 ASIC 아키텍처를 통해 업계 최고 수준의 위협 보호 및 복호화 기능을 고성능으로 제공합니다. 또한 SD-WAN, 스위칭 및 무선, 5G와 같은 통합 기능을 통해 보안 네트워킹을 제공합니다. 보안 및 네트워킹 포인트 솔루션을 단일 운영 체제인 FortiOS 기반의 중앙 집중식 관리 콘솔로 통합하여 관리합니다.

솔루션별 특장점

AI/ML 보안

포티넷의 광범위한 포트폴리오에 있는 보안 솔루션과 통합되어 애플리케이션, 콘텐츠, 웹 트래픽, 장치 및 사용자를 어디서나 보호하는 시장 선도적인 보안 기능을 제공합니다.

The ASIC

보안 장치가 네트워크 및 보안 아키텍처 내에서 성능 병목 현상이 되어서는 안 되며, 필요한 차세대 방화벽의 성능 향상을 위해 지속적으로 혁신하고 새로운 보안 처리 장치(SPU)를 개발하고 있습니다.

단일 OS 플랫폼

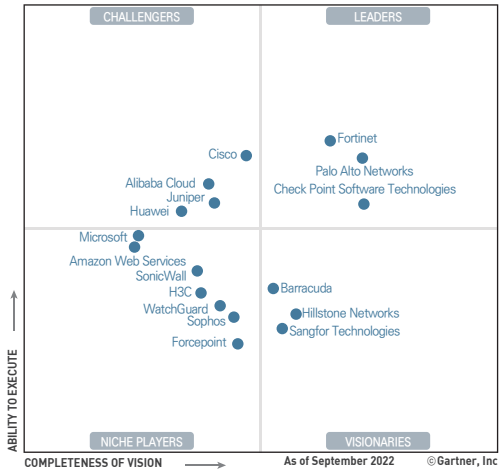
FortiOS를 사용하여 온프레미스, 클라우드, 하이브리드, 융합 IT / OT / IoT 인프라를 포함한 모든 환경에서 일관된 사용자 경험, 공통 보안 정책, 가시성 및 제어를 수행합니다.

SD-WAN 통합기능

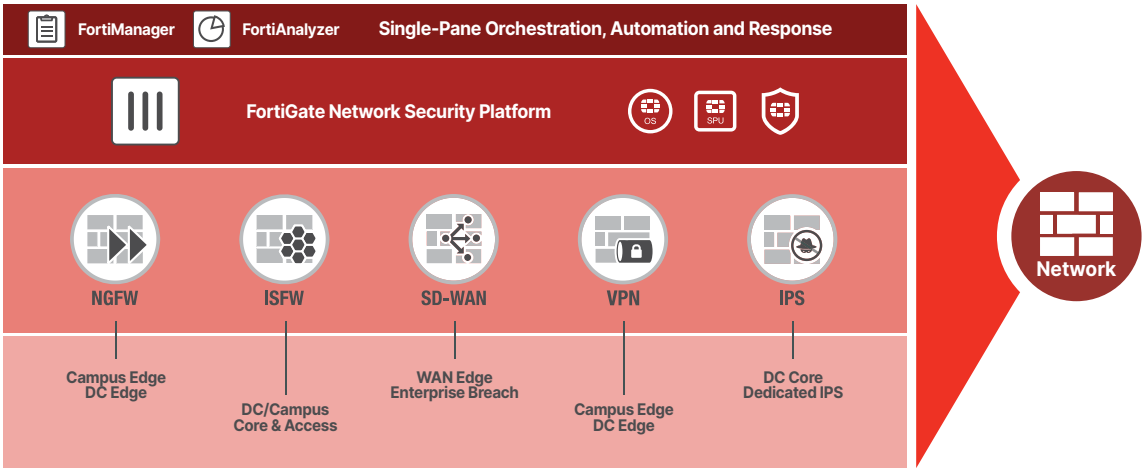
FortiOS 플랫폼을 활용하여 단일 플랫폼에서 SD-WAN 기능을 포함하여 제공합니다. 최신 트렌드인 SASE 관점에서 보더라도, 서비스 에지 기능 및 보안 기능의 통합은 차세대 방화벽의 보안을 더욱 강화해 줍니다.

Why FORTINET ?

2022년 Gartner® Magic Quadrant™
네트워크 방화벽 부문 13년 연속 Leader로 선정



이 솔루션을 어떻게 써야 하나요?



포티넷 보안 패브릭의 핵심 요소인 FortiGate NGFW는
점점 가속화되는 고성능 엔터프라이즈 네트워킹의 요구에 부합하는 보호 기능을 제공합니다.

포티넷 ATP 솔루션

포티넷의 샌드박싱 솔루션은 제로데이 멀웨어 및 기타 지능형 파일 기반 위협을 탐지하고 분석합니다. 포티가드 AI 기반 인라인 멀웨어 방지 서비스는 업계 최초로 NGFW에서 인라인 차단을 제공합니다. PaaS, SaaS, 가상 머신, 어플라이언스 등 다양한 경우의 유연한 배포를 가능하게 합니다.

솔루션별 특장점

지능형 멀웨어 탐지 및 대응

즉각적인 위협 대응을 위해 실시간으로 위협 인텔리전스를 공유하고, 부족한 보안 리소스에 대한 의존도를 낮추는 과정을 자동화합니다.

인증 및 최고의 성능

제3자 기관을 통해 독립 테스트를 지속적으로 거치고 있으며, 알려진 위협과 알려지지 않은 위협에 대처하는 데 있어 계속해서 최고 수준의 등급을 받고 있습니다.

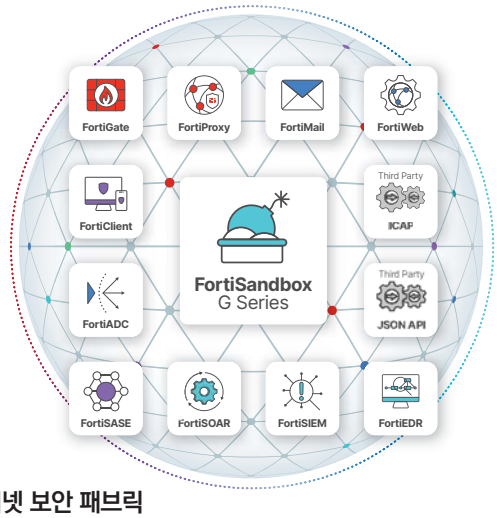
Mitre ATT&CK 기반 보고 및 조사 도구

FortiSandbox는 발견된 멀웨어 기술을 판별하는 세부적인 분석 보고서를 Mitre ATT&CK 프레임워크에 제공합니다.

AI 기반의 샌드박스 멀웨어 분석

제로데이 위협에 대해 더 효율적이고 효과적으로 만드는 행동 기반 AI를 활용하여 전체 공격 라이프사이클을 파악하기 위해 통제된 환경에서 수행됩니다.

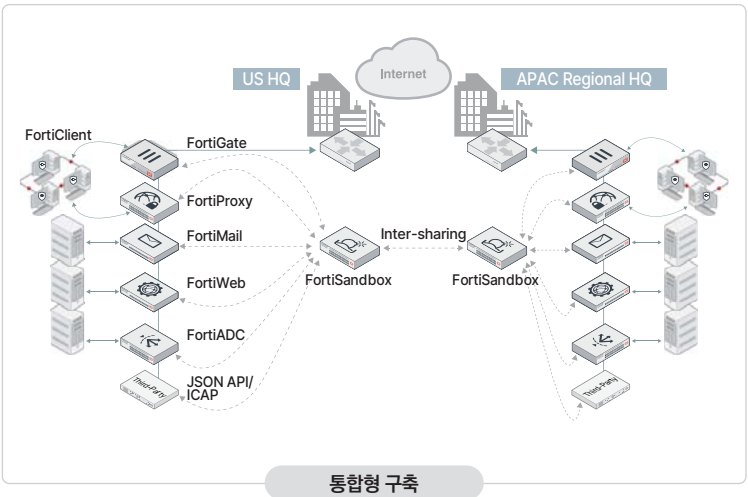
Why FORTINET ?



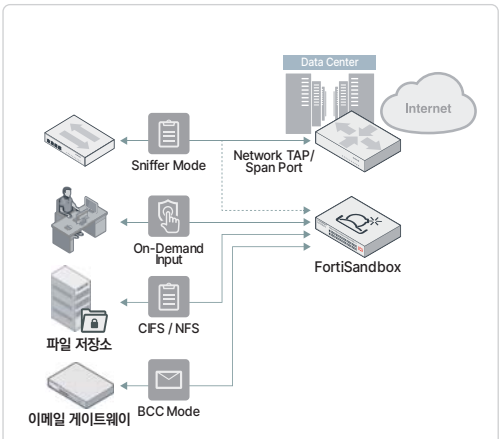
포티넷 보안 패브릭

다양한 제품들과 연동되며 포티넷 보안패브릭을 통해 통합 보안을 가능하게 합니다.

이 솔루션을 어떻게 써야 하나요?



통합형 구축



독립형 구축

FortiSandbox는 고객의 다양한 요구 사항에 대해 유연한 구축 옵션을 제공합니다.

포티넷 CASB 솔루션

FortiCASB는 SaaS 어플리케이션에 대한 가시성을 제공하고 동시에 차단 기능을 제공합니다. 사용 중인 SaaS 애플리케이션에 대해서 사용자 기반의 어플리케이션 및 데이터를 종합적으로 보호합니다.

솔루션별 특장점

온디맨드 데이터 스캔

프록시 기반 서비스나 하드웨어 기기와 달리, SaaS 제공 업체에 직접 연결하여 기업 계정에 저장된 데이터와 파일에 직접 액세스합니다.

사용자 인사이트 및 정책

FortiCASB는 클라우드 기반 애플리케이션에서 사용자 행동과 활동에 인사이트를 제공하는 다양한 도구가 갖춰져 있습니다.

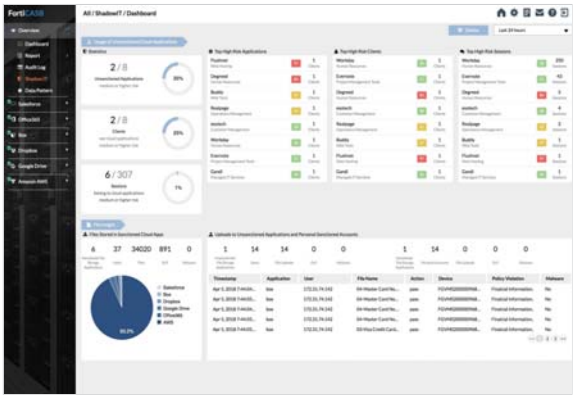
규정 준수 및 DLP

FortiCASB는 데이터 보호를 위한 다양한 정책과 도구를 제공하고, 각종 컴플라이언스에 대응하는 자동 보고서 기능을 제공합니다.

FortiGuard와의 통합

FortiGuard 안티바이러스 서비스가 기본으로 포함되어 있어서 클라우드에 저장된 파일을 스캔할 수 있습니다. 이 서비스는 추가 비용 없이 FortiCASB 구독자에게 제공됩니다.

Why FORTINET ?



포티넷 ZTNA와 SASE도 동시에 지원

FortiGate ZTNA Access Proxy 기능을 활용하여 CASB를 지원합니다. 또한 SASE의 경우 어플리케이션 및 SSL 복호화 기능을 포함하여 CASB 기능을 심층적으로 지원합니다.

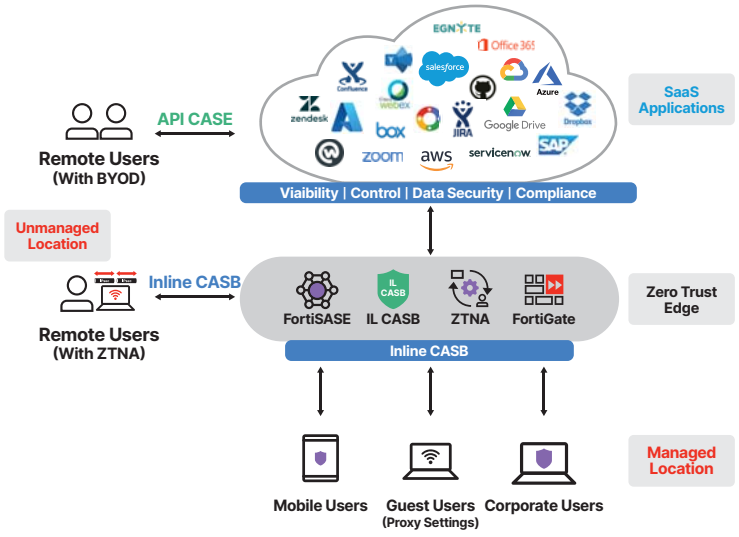
이 솔루션을 어떻게 써야 하나요?

Inline 혹은 API 기반의 구성

포티넷의 ZTNA나 SASE 기술과 인라인으로 직접 연동하거나, SaaS 어플리케이션에 대해서 직접 API로 연동합니다.

주요 클라우드 제공업체 지원

FortiCASB는 Microsoft Office 365 OneDrive, Google Drive, Salesforce.com, Dropbox, Box를 비롯한 주요 SaaS 및 클라우드 서비스와의 완전한 API 통합을 통해 사용이 가능합니다.



포티넷 클라우드 워크로드 보안 솔루션

FortiCNP(Cloud-Native Protection) 는 기본적으로 클라우드 서비스 제공 업체의 보안 서비스 및 포티넷 보안 패브릭과 통합되어 포괄적인 풀스택 클라우드 보안 솔루션을 제공합니다. FortiCNP의 특허받은 Risk Resource Insights(RRI) TM 기술은 분석 결과를 맥락화하고 실행 가능한 인사이트를 통해 가장 중요한 것의 우선순위를 지정하여 보안을 간소화함으로써 팀이 클라우드 위험을 효과적으로 관리할 수 있도록 지원합니다.

솔루션별 특장점

중앙 집중화된 가시성

FortiCNP는 다중 클라우드 환경에서 중앙 집중화된 가시성과 보고 기능을 제공합니다. FortiCNP는 보안 상태를 한눈에 쉽게 알아볼 수 있도록 대시보드, 로그 및 보고서를 제공합니다.

온디맨드 데이터 스캔

FortiCNP는 프록시 기반 서비스나 하드웨어 디바이스와는 달리 클라우드 제공 업체에 직접 연결하여 기업의 계정에 보관된 데이터 및 파일에 액세스 합니다.

사용자 인사이트 및 정책

FortiCNP는 다양한 도구를 제공하여 클라우드 기반 애플리케이션에서 일어나는 사용자 동작과 활동에 관한 인사이트를 얻을 수 있습니다.

위협 보호 및 대응

FortiCNP는 UEBA(User Entity Behavior Analytics)를 사용하여 의심스럽거나 변칙적인 사용자 동작을 찾습니다. 또한, 악성 동작이 발견되면 경고를 보냅니다.

Why FORTINET ?

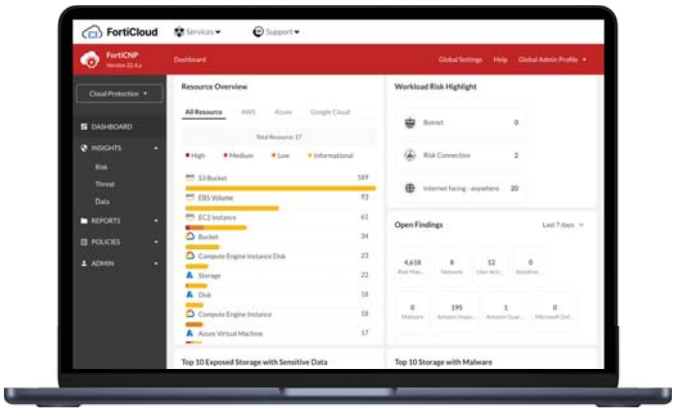
실행 가능한 인사이트를 통한 클라우드 위험 관리

FortiCNP는 여러 보안 서비스와 경고를 분석하여 가장 위험이 높은 리소스에 대한 실행 가능한 인사이트를 제공하여 보안 팀은 중요한 업무에 집중할 수 있습니다.

이 솔루션을 어떻게 써야 하나요?

주요 활용 방안 및 기능

- 클라우드 보안 위험 우선순위 지정
- 취약성 관리
- 클라우드 보안 자세 관리
- 악성코드 검사
- 클라우드 네이티브 보안 통합
- 워크플로우 통합



포티넷 통합 정책 관리 솔루션

FortiManager는 단일 콘솔에서 자동화 기반 중앙 집중식 관리를 제공합니다. 이 프로세스를 통해 간소화된 프로비저닝과 혁신적인 자동화 도구를 통해 네트워크 장치에 대한 전체 관리 및 가시성을 확보할 수 있습니다. 특히 SD-WAN의 대규모 배포를 위한 템플릿을 통한 제로 터치 프로비저닝을 제공하고, 포티넷 보안 패브릭과 500개 이상의 에코시스템 파트너와의 통합 연동 기능도 제공합니다.

솔루션별 특장점

단일 콘솔 관리 및 프로비저닝

단일 콘솔 관리 및 프로비저닝은 역할 분리와 중앙 집중식 정책을 통해 방화벽 관리 및 IPS 관리를 단순화합니다.

패브릭 자동화

패브릭 자동화(Fabric Automation)는 다양한 환경의 유연한 프로비저닝을 위해 SD-Branch에 대한 제로 터치 프로비저닝을 제공합니다.

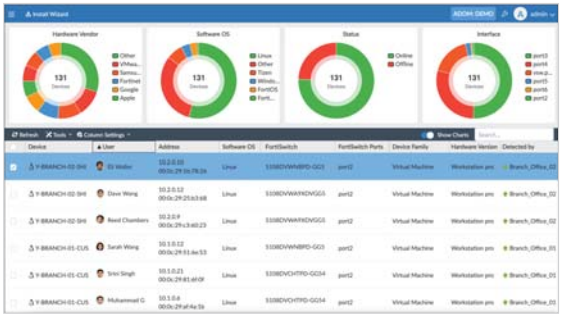
모니터링 및 가시성 문제 해결

연결 관련 문제를 해결하기 위한 속도 테스트와 LAN 관련 문제를 조사하기 위한 패킷 캡처 기능이 내장되어 있습니다.

하이브리드 환경의 Mesh 방화벽

포티넷은 복잡한 하이브리드 환경 전반에서 일관된 보안을 설정할 수 있는 중앙 집중식 통합 관리를 제공하는 유일한 벤더입니다. 중앙 집중식 통합 관리는 온프레미스 및 클라우드에 구축된 포티게이트 차세대 방화벽은 물론, SD-WAN, 보안 WLAN/LAN, 범용 ZTNA, 포티SASE를 포괄합니다.

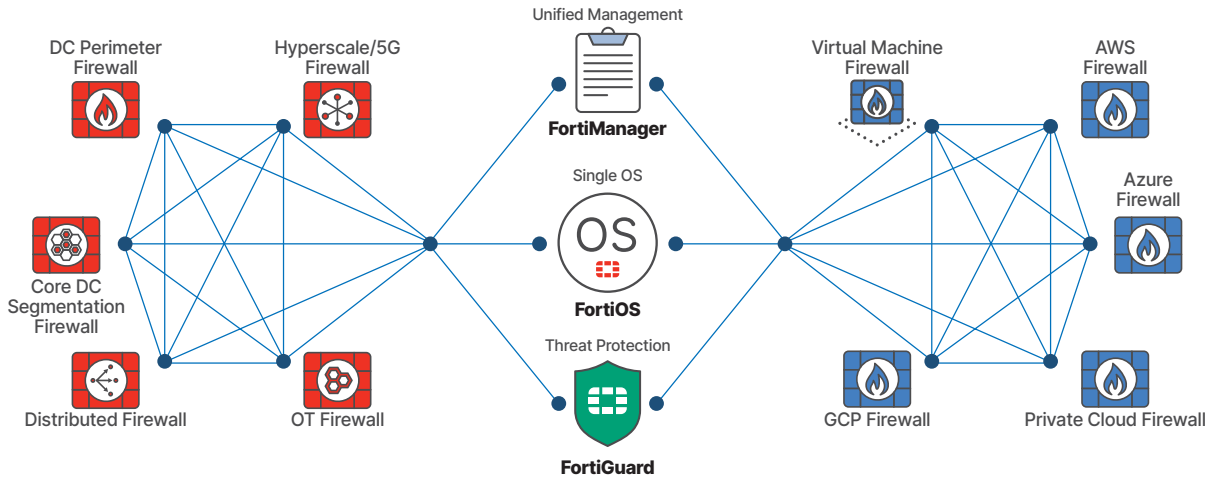
Why FORTINET ?



중앙 집중화된 보안 정책 관리

FortiManager의 관리 콘솔은 간소화된 '단일 창' 환경을 제공하여 탁월한 네트워크 인사이트를 제공합니다. 연결성, 리소스 사용률, 장치 설정, 정책 상태, 알림을 포괄합니다. 또한 다양한 폼 팩터에 걸쳐 포티게이트를 손쉽게 조율하는 동시에 강력한 관리 기능을 포티스위치, 포티AP, 포티익스텐더를 포함한 전체 포티OS 기반 네트워킹 에코시스템으로 확장합니다. 이러한 통합은 조직 네트워크 전체에 걸쳐 통합 보안 정책을 일관되게 적용하여 보안을 강화하고 관리를 간소화하여 최적의 성능을 보장합니다.

이 솔루션을 어떻게 써야 하나요?



FortiManager는 복잡한 하이브리드 환경에서 일관된 보안을 위해 통합 관리를 제공하여 보안 위협으로부터 보호합니다.

포티넷 시큐어 웹 게이트웨이 솔루션

FortiProxy는 인터넷 기반 공격으로부터 내부 사용자를 보호합니다. URL 필터링, DLP, 애플리케이션 가시성 및 제어, 안티바이러스, 침입 방지, 콘텐츠 분석, 고성능 SSL 복호화, 클라이언트 브라우저 격리 등 중요한 기능을 15Gbps 프록시 속도와 500~50,000명의 사용자를 동시에 수용하여 하나의 장비에서 구현 가능합니다.

솔루션별 특장점

고급 SSL 검사

SSL 검사를 실행하고 성능 저하 없이 암호화된 트래픽에서 사각지대를 효과적으로 제거하는 강력한 하드웨어입니다.

보안 패브릭

FortiProxy는 FortiSandbox, FortiAnalyzer 등의 주요 보안 패브릭 구성 요소와 통합됩니다. 또한, ICAP와 WCCP 프로토콜을 사용하여 타사 보안 기기와 통합할 수도 있습니다.

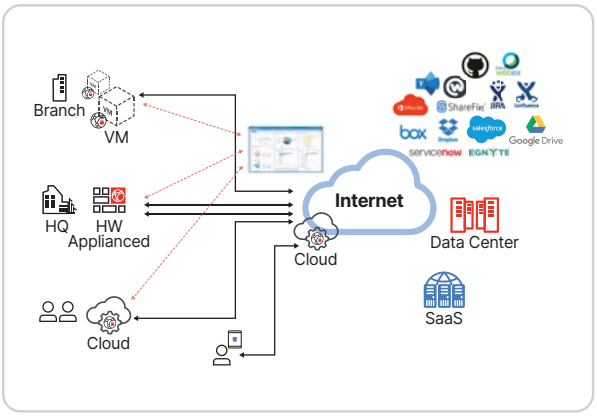
고성능, 확장성 및 낮은 TCO

FortiProxy는 최대 15Gbps에 이르는 프록시 속도를 지원하며, 사용자가 500명인 소규모 기업부터 최대 5만 명인 대기업까지 확장할 수 있습니다.

AI 기반의 보안 서비스

모든 환경에 맞게 확장 가능한 지능형 보안 기능으로 사용자를 보호합니다.

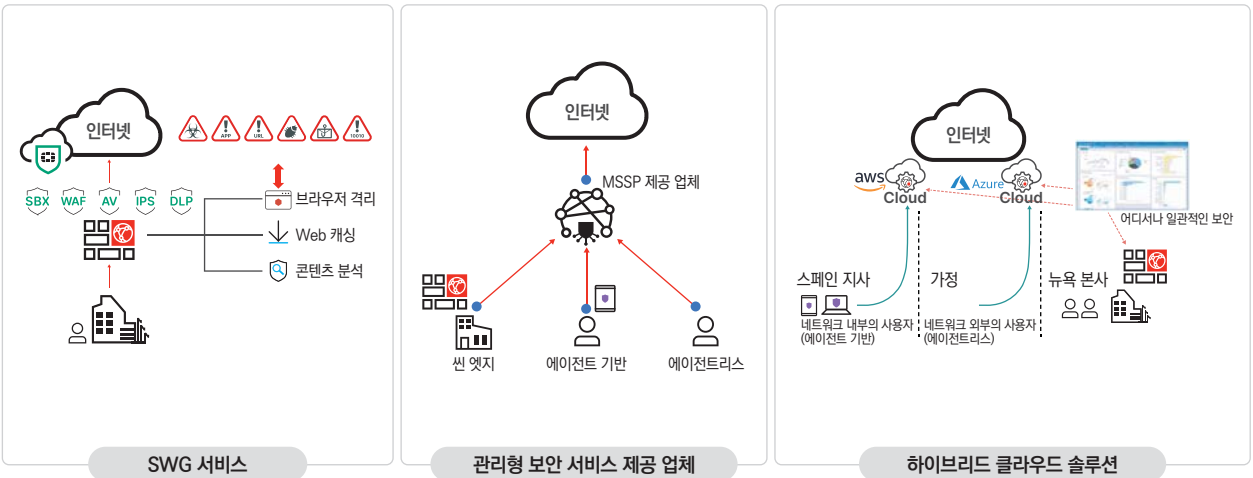
Why FORTINET ?



강력한 가시성과 보안

FortiProxy는 다양한 포티가드 서비스 및 각종 보안 기능을 활용하여 최신 웹 위협으로부터 사용자를 보호하고 규정 준수를 강화합니다.

이 솔루션을 어떻게 써야 하나요?



FortiProxy는 업계에서 가격 대비 가장 높은 성능을 제공합니다.

포티넷 이메일 보안 솔루션

FortiMail은 피싱, 랜섬웨어, 제로데이, 비즈니스 이메일 침해(BEC) 공격과 같은 모든 이메일 기반 위협으로부터 기업을 보호합니다. 포티메일 솔루션은 포티가드랩에서 개발한 포티가드 AI 기반 보안 서비스를 활용하여 이메일 기반 위협을 실시간으로 예방, 탐지 및 대응하는 최첨단 보안 기술을 제공합니다.

솔루션별 특장점

이메일 매개 위협으로부터 보호

강력한 스팸 방지 및 멀웨어 방지 기능은 원치 않는 대량 이메일, 피싱, 랜섬웨어, 비즈니스 이메일 손상 및 표적 공격을 차단합니다.

검증된 성능

Fortinet은 독립적인 테스트를 통해 FortiMail의 효율성을 지속적으로 입증하는 유일한 이메일 보안 공급업체 중 하나입니다. SE Labs로부터 AAA 등급을 받았고 Virus Bulletin으로부터 99.97%의 스팸 탐지율을 기록했습니다.

패브릭 지원 이메일 보안

FortiMail은 Fortinet 제품 및 타사 구성 요소와 통합되어, 매끄럽게 운영되는 보안 패브릭 전반에서 IoC를 공유함으로써 보안에 대한 사전 예방적 접근 방식을 채택할 수 있도록 지원합니다.

FortiGuard Labs와 연동

전 세계 60만 개의 고객 환경에 대한 가시성을 확보하고 있는 FortiGuard Labs는 현존하는 최고의 위협 연구팀 중 하나입니다.

Why FORTINET ?

99.97%
스팸 탐지율

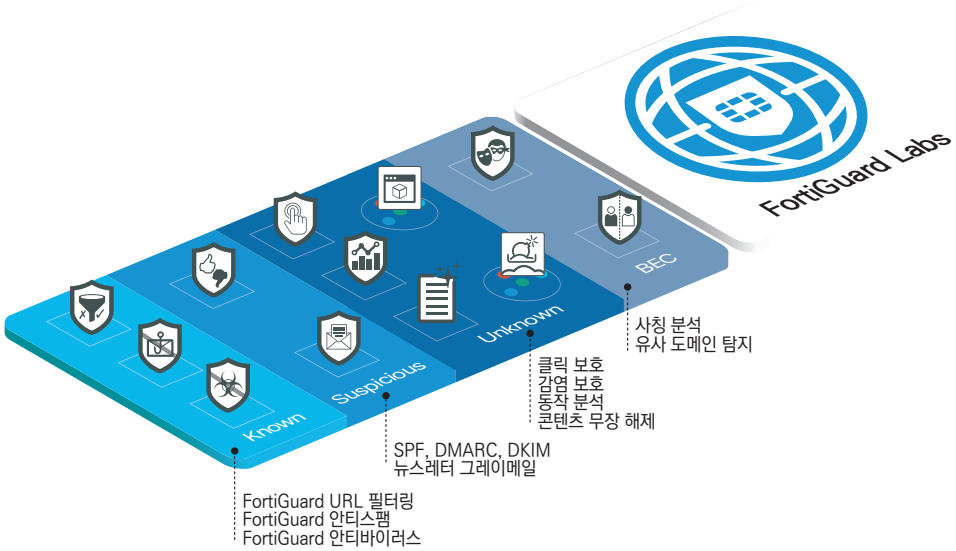
100%
멀웨어 탐지

97%
전체 탐지율

업계에서 인정받는 최고의 성능

FortiMail은 독립적인 타사 테스터가 측정한 결과 우수한 성능을 제공합니다.

이 솔루션을 어떻게 써야 하나요?



FortiMail은 이메일이 기업에 가하는 위험을 해결하며, 최신 위협에 대한 FortiGuard Labs의 글로벌 가시성과 인텔리전스를 통해 더욱 강화됩니다.

포티넷 엔드포인트 보안 솔루션

FortiEDR은 유연한 배포 옵션과 예측 가능한 운영 비용으로 단일 통합 플랫폼에서 현재 및 기존 운영 체제는 물론 제조 및 OT 시스템을 갖춘 워크스테이션과 서버를 비롯한 모든 통신 장치에 대하여 설정된 사고 대응을 통해 실시간 자동 엔드포인트 보호 기능을 제공합니다.

솔루션별 특장점

실시간 사전 예방 위험 완화 및 IoT 보안

각종 사이버 공격을 사전에 감지하고 예방 조치를 가능하게 합니다. 예를 들어 취약성 평가 및 사전 예방적 위험 완화 기반 정책 등 취약점이 있는 것으로 알려진 모든 애플리케이션의 통신 관리도 지원합니다 .

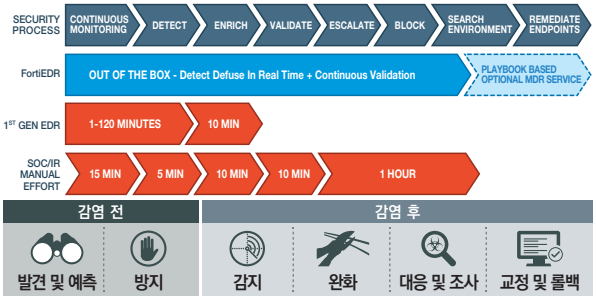
사전 보호

파일 기반 멀웨어의 감염을 방지하는 맞춤형 커널 레벨 차세대 머신러닝 기반 안티바이러스(NGAV) 엔진을 통해 1차 방어선을 제공합니다.

사후 보호

FortiEDR은 엔드포인트가 손상된 경우에도 지능형 공격을 실시간으로 탐지하고 중지하는 유일한 솔루션입니다. 피해가 발생하지 않고, 데이터가 손실되지 않으며, 아무런 문제가 없습니다.

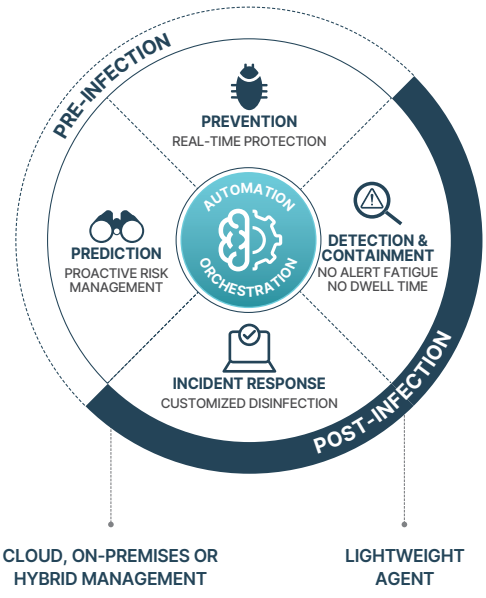
Why FORTINET ?



포괄적인 엔드포인트 보안 플랫폼

FortiEDR은 지능형 위협을 탐지하고 이미 손상된 장치에서도 실시간으로 침해 및 랜섬웨어 피해를 막음으로써 자동으로 사고에 대응하고 해결하여 데이터를 보호하고, 시스템 가동 시간을 보장하며, 비즈니스 연속성을 유지하도록 처음부터 제작된 유일한 엔드포인트 보안 솔루션입니다.

이 솔루션을 어떻게 써야 하나요?



지원되는 플랫폼

- Windows XP SP2/SP3, 7, 8.x 및 10.x, Windows Server 2003 R2, 2008 R1, 2008 R2, 2012, 2012 R2, 2016, 2019
- macOS Yosemite(10.10), El Capitan(10.11), Sierra(10.12), High Sierra(10.13), Mojave(10.14), Catalina(10.15)
- VDI 환경: VMware Horizons 6 및 Citrix XenDesktop/XenApp
- Red Hat Enterprise Linux 6.8, 6.9, 6.10 및 7.x
- CentOS 6.8, 6.9, 6.10 및 7.x
- Ubuntu 16.04, 18.04

무겁지 않은 경량 EDR

FortiEDR은 강력한 차단 및 제어기능을 가지고 있으면서 사용자 환경의 리소스를 최소한으로 사용하도록 디자인 되었습니다.

포티넷 유무선 LAN 인프라 솔루션

Fortinet LAN 엣지 솔루션은 업계 최고의 FortiGate로 네트워크 관리를 통합합니다. 이를 통해 포괄적인 LAN 인프라 보안과 일상적 관리 단순화를 달성할 수 있습니다. Fortinet은 내장된 모범 사례 구성을 통해 최소한의 기술 전문성으로 대규모 네트워크를 배포할 수 있도록 지원합니다.

솔루션별 특장점

유무선 네트워크

안정적으로 특수 설계된 고성능 포티넷 이더넷 스위치 및 무선 액세스 포인트는 차세대 캠퍼스에 필요한 사용자 경험을 안전하게 운영해 줍니다.

보안

포티넷은 보안과 네트워크를 하나의 플랫폼에 융합하여 매우 안전한 유무선 솔루션을 제공합니다.

순화된 관리 및 자동화

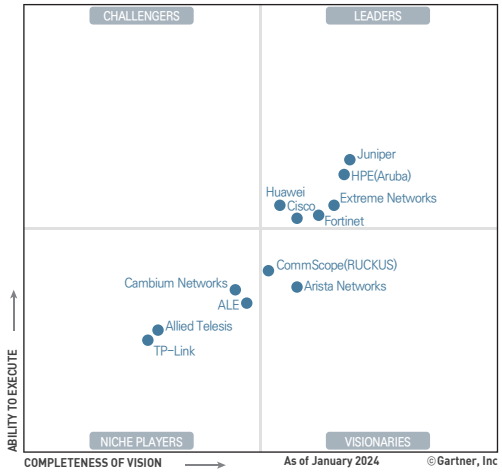
안정적인 NOC와 프로비저닝을 제공하는 포티넷은 하나의 캠퍼스 및 멀티 캠퍼스 환경을 지원하도록 확장할 수 있습니다.

인공 지능(AI)과 머신 러닝(ML)

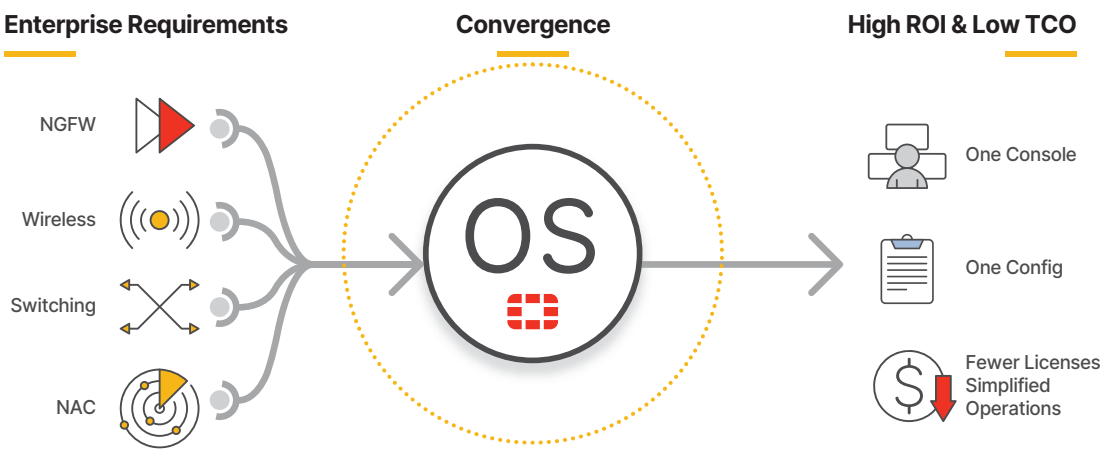
AI 및 ML은 IT팀에게서 반복적인 작업의 부담을 줄여주면서도 트렌드와 네트워크 상태에 대한 알림을 보내 캠퍼스 네트워크를 미리 관리할 수 있도록 합니다.

Why FORTINET ?

2024년 Gartner® Magic Quadrant™
LAN 인프라 부문 Leader로 선정



이 솔루션을 어떻게 써야 하나요?



유무선 인프라, 엔드포인트를 하나의 플랫폼에서 관리하여 운영 효율은 높이고 비용은 낮춥니다.

포티넷 SOC 플랫폼

보안을 위한 통합 이벤트 관리 및 상관관계 분석을 위한 SIEM 그리고 자동화 관점의 SOAR를 협업 모델로 제공하여 효과적인 SOC팀의 업무포털을 제공합니다.

솔루션별 특장점

FortiSIEM

- 각종 로그 및 데이터에 대한 신속한 통합 및 확장성을 제공합니다.
- 자동화된 워크플로우를 통한 효과적인 정책이 가능합니다.
- 강력한 자산관리 기능을 포함합니다.
- 각 모듈별 유연한 확장성을 제공합니다.

FortiSOAR

- 자동화를 위한 유연한 플레이북을 지원합니다.
- Incident Response를 위한 플랫폼을 제공합니다.
- 각종 인텔리전스 데이터 및 과거 업무처리 내역을 통합 관리하여 우리 회사를 위한 자체 통합 인텔리전스를 구성합니다.

SOC 업무 포탈

- SIEM에서 생성된 이벤트를 SOAR를 통해서 체계적으로 인시던트화 하여 관리를 수행합니다.
- 자동화 및 오케스트레이션을 통하여 발생된 보안 사고를 직접적이고 능동적으로 대처합니다.
- 보안팀의 콜라보레이션 각종 통합 기능을 활용하여 SOC의 인력 부담을 줄여줍니다.

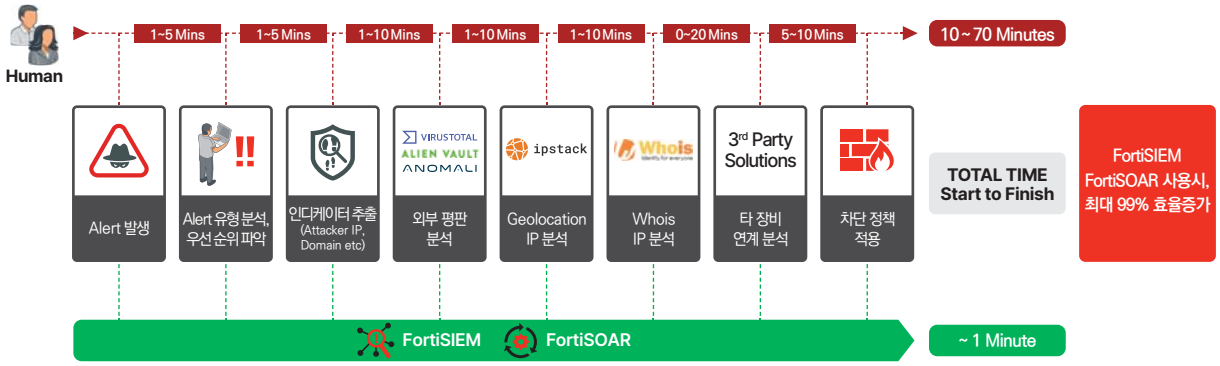
Why FORTINET ?

포티넷 SOC 리더쉽 보드

2023 KuppingerCole Leadership Compass SOAR부분 Leader 선정

2023 GigaOm Radar SOAR부분 Leader 선정

이 솔루션을 어떻게 써야 하나요?



FortiSIEM통한 각종 이벤트의 효과적인 상관관계분석을 통한 인시던스 도출 정재된 이벤트를 기반으로 FortiSOAR에서 효과적인 자동화 수행, 궁극적으로 SOC 업무 통합

포티넷 ICS/OT 보안 솔루션

Fortinet은 10년 이상 에너지, 방위, 제조, 식품 및 운송과 같은 중요 인프라 부문에서 OT 환경을 보호해 왔습니다. Fortinet 보안 패브릭을 통해 복잡한 인프라에 보안을 설계함으로써 조직은 OT 환경을 보호하고 규정을 준수하는 효율적이고 지속적인 방법을 보유하게 됩니다.

솔루션별 특장점

혹독한 산업환경을 위한 네트워크 보안 솔루션

혹독한 산업환경에서 사용 가능한 Rugged Type 방화벽과 스위치 및 액세스 포인트, 디지털 고스트를 구현하는 FortiDeceptor 제품은 실외에서 사용하거나, 온도가 높거나 낮은 환경에서 사용이 가능하도록 제작되었습니다.

전문화된 OT 위협 인텔리전스

Fortinet은 다양한 산업 환경에서 사용하는 산업 표준 프로토콜과 ICS 벤더사의 독점 프로토콜을 사용하는 통신을 감지할 수 있도록 Application Signature를 3,000개 이상 제공하고 있습니다.

OT 경험이 풍부한 전담팀

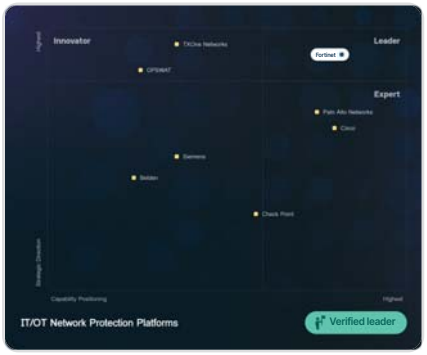
Fortinet의 산업 전문 지식은 석유 및 가스, 운송, 에너지, 전력 및 유틸리티, 제조 등의 산업에서 요구하는 고유한 사이버 보안 요구 사항에 대해 검증된 지원을 제공합니다.

광범위하고 통합된 생태계

Fortinet의 개방형 생태계 접근 방식은 보안 패브릭의 이점을 Fortinet이 개발한 패브릭 커넥터를 통해 고유한 OT 패브릭 지원 파트너 솔루션으로 확장하고, 패브릭 API 및 DevOps 도구를 통해 다른 파트너 솔루션으로 확장합니다.

Why FORTINET ?

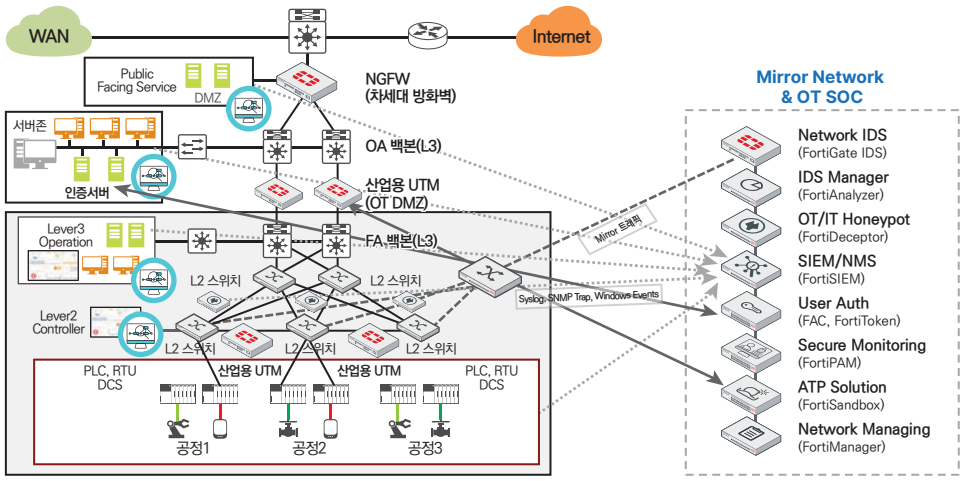
2023 IT/OT Network Protection Platform 분야에서
2년 연속 리더로 선정된 유일한 기업



유일하게 리더(Leader) 등급으로 평가받은 포티넷은 다양한 산업 환경에서 필요로 하는 보안 솔루션을 플랫폼으로 제공하고 있으며 대규모의 고객 기반과 강력한 커버리지를 보유하고 있습니다.

포티넷의 통합형 OT 인지 보안 패브릭 플랫폼을 통해 중요한 OT 자산을 보호하십시오.

이 솔루션을 어떻게 써야 하나요?



- ☑ 다양한 환경조건에서도 LAN Extension 또는 보안 가시성을 확보합니다.
- ☑ 관리되지 못했던 내부 구간을 플랫폼 기반의 OT 보안 제품으로 관리합니다.
- ☑ 원격지의 위협에 선제적으로 대응할 수 있도록 디지털 고스트를 활용합니다.

포티넷 시큐어 SD-WAN 솔루션

Fortinet 시큐어 SD-WAN은 보안에 민감한 클라우드 우선 글로벌 기업과 하이브리드 인력을 지원합니다. 당사의 보안 네트워킹은 하나의 운영 체제를 사용하고 SD-WAN, 차세대 방화벽(NGFW), 고급 라우팅 및 ZTNA, 애플리케이션 게이트웨이 기능을 통합하였습니다.

솔루션별 특장점

더 나은 애플리케이션 경험

SD-WAN은 원격 사이트가 네트워크, 데이터 센터 및 또는 다중 클라우드 기반 시스템에 보다 쉽게 연결될 수 있도록 해 주며, 대기 시간이 짧고 성능이 더 우수하며 연결이 보다 안정적입니다.

즉각적인 ROI 혜택

SD-WAN 장점은 대역폭 비용을 크게 절감할 뿐만 아니라 에지에서 다양한 포인트 네트워킹 및 보안 제품을 통합하는 동시에 더 나은 제어 및 성능을 제공함으로써 비용을 절감하는 데 도움이 될 수도 있습니다.

효율적인 운영

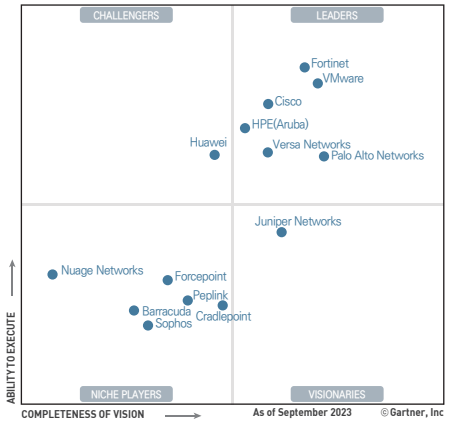
SD-WAN은 중앙 집중식 오케스트레이션, 제로 터치 프로비저닝 및 분석과 더불어 클라우드 온램프의 심층적인 통합을 지원하여 클라우드 연결을 가속화합니다.

강화된 보안 태세

SD-WAN은 FortiManager 및 FortiAnalyzer와 함께 네트워크 트래픽에 대한 세부적인 가시성을 제공하고 트래픽 데이터를 분석하며 해당 결과에 따라 대응을 자동화합니다.

Why FORTINET ?

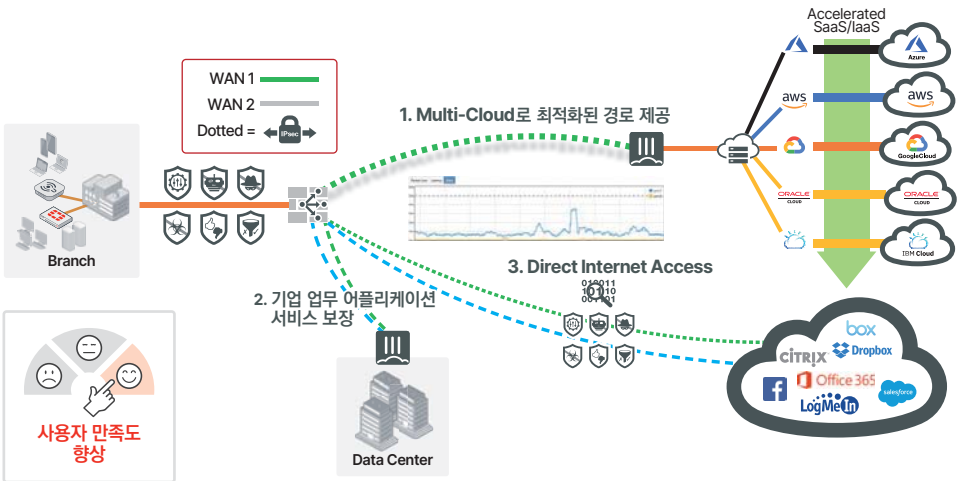
2023년 Gartner® Magic Quadrant™
SD-WAN 부문 Leader로 선정



3년 연속으로 실행 능력 최상위 평가를 받은 공급업체는 업계에 오직 포티넷뿐입니다. 게다가 4년 연속 리더로 선정되는 영예도 차지했습니다. 이것은 포티넷의 혁신적인 보안 SD-WAN 솔루션 덕분입니다.

포티넷 시큐어 SD-WAN은 세계적으로 신뢰받고 있는 솔루션입니다.

이 솔루션을 어떻게 써야 하나요?



- ☑ 최적의 WAN 회선으로 통신하게 하여 애플리케이션 속도를 높입니다.
- ☑ 중요 서비스의 우선순위를 높여 서비스를 보장합니다.
- ☑ 보안 기능(AV, IPS)을 통해 내부망에 대한 보안성을 높입니다.

포티넷 ZTNA 솔루션

Fortinet 범용 ZTNA는 위치에 관계없이 어디서나 작업하는 사용자에게 안전하고 간단한 애플리케이션 액세스를 제공합니다.

솔루션별 특장점

유연한 배포

원격 근무자와 현장 근무자 모두에게 동일한 보안 정책을 적용시켜 통일성과 관리의 편리함을 동시에 제공합니다.

지속적인 검증

애플리케이션의 액세스 권한을 부여하기 전에 사용자 ID, 기기 ID, 기기 상태를 확인하며, 권한을 부여한 후에도 지속적으로 엔드포인트 상태를 확인합니다.

통합 FortiClient 에이전트

단일 에이전트를 위해 VPN, ZTNA, 취약성 검색, URL과 애플리케이션 필터링 및 엔드포인트 보호를 제공합니다.

자동 암호화 터널

엔드포인트와 액세스 프록시 간에 TLS 암호화를 자동으로 설정하여 트래픽을 숨기는 것이 가능합니다.

Why FORTINET ?

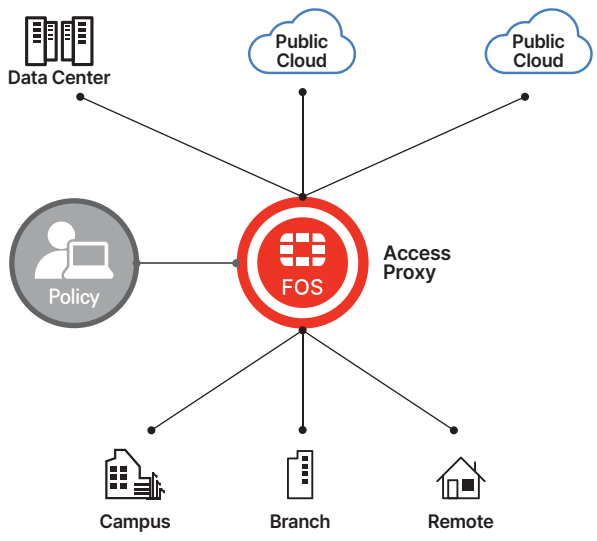
포티넷 ZTNA만의 특징

- Cloud 또는 온프레미스 배포 모두에서 고유한 확장성과 유연성 확보
- 보안 검사를 적용할 수 있는 저지연 아키텍처를 제공
- 운영 체제에 통합되어 있어 ZTNA를 쉽게 구현 가능
- SASE 구매 없이 FortiClient EMS를 통해 ZTNA 서비스 가능

포티넷 보안 패브릭

다양한 제품들과 연동되며 포티넷 보안패브릭을 통해 광범위한 공격면을 보호합니다.

이 솔루션을 어떻게 써야 하나요?



VPN 대체

ZTNA 솔루션을 통해 VPN 없이 보안 정책을 적용한 Access 제어를 합니다.

안전하고 세분화된 제어

디바이스 확인을 통해 사용자를 애플리케이션 Role 기반으로 세분화합니다.

장소에 제한되지 않은 사용자 제어

온프레미스, 지점, 원격 클라우드, 퍼블릭 클라우드 등 내/외부에서 접근하는 사용자 제어

포티넷 Unified SASE 솔루션

클라우드 및 하이브리드 환경의 업무 환경의 모든 사용자와 어플리케이션을 단일 운영체제, 단일 오케스트레이션 및 통합 엔드포인트 에이전트 그리고 AI 기반 보안서비스로 보호합니다.

솔루션별 특장점

하나의 운영 체제

접속환경의 주요 인프라를 하나의 FortiOS로 구현하여 높은 가용성과 유연한 확장성을 보장합니다.

통합 관리 플레인

SaaS 기반의 통합 매니지먼트의 제공을 통해 로그에 대한 기본적인 검색 및 분석 그리고 대쉬보드 기능 등을 제공합니다.

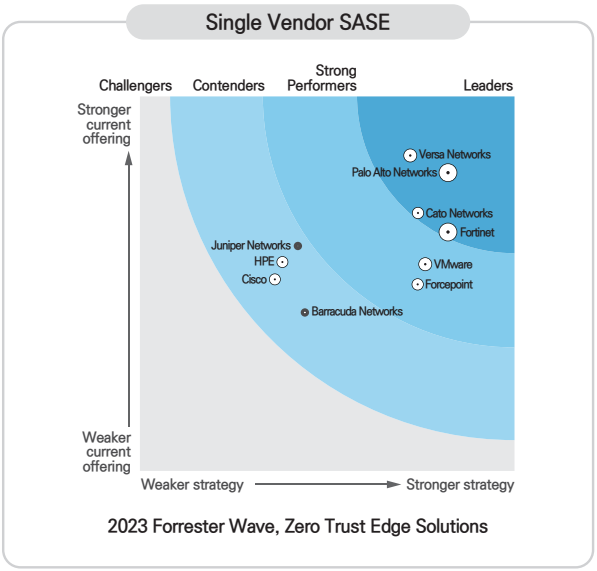
하나의 분석 엔진

단순 Data Lake의 범주를 넘어서서 포티넷의 보안 전문가가 SoC서비스의 제공도 가능합니다.

통합 엔드포인트 에이전트

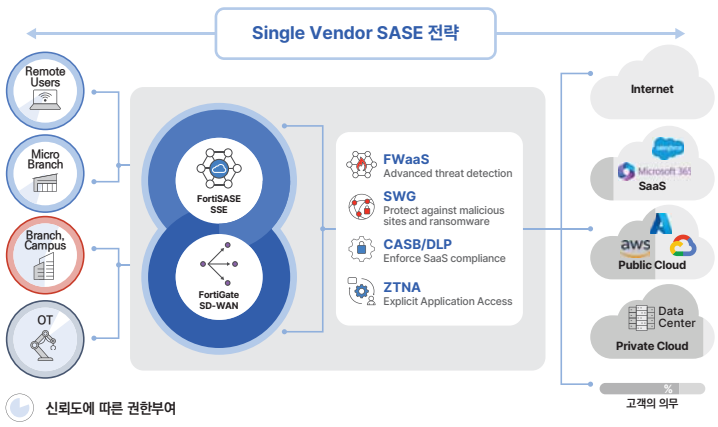
온프레미스, 클라우드를 포함하여 경량화된 통합 엔드포인트 에이전트를 통하여 제로트러스트 환경의 구성이 가능합니다.

Why FORTINET ?

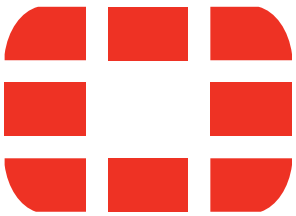


2023 Forrester Wave, Zero Trust Edge Solutions

이 솔루션을 어떻게 써야 하나요?



- 전용 클라이언트 혹은 포티게이트 장비를 활용하여 안전하게 사용자와 어플리케이션을 보호합니다.
- 프락시, 방화벽, DLP, CASB, 샌드박스 등의 각종 보안 기능을 기본적으로 제공합니다.
- 포티넷 분석팀을 통해서 DEM, 엔드포인트 포렌식을 포함한 보안관제서비스도 제공합니다.



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