FORTINET

INTRODUCE

포티넷 회사소개서

목차

포티넷 회사소개 3

포티넷 시큐리티 패브릭 4

포티넷 코리아 고객 솔루션 체험 센터 소개 5

포티넷 주요 솔루션 소개

- 차세대 방화벽 6
- ATP 솔루션 7
- CASB 솔루션 8
- 클라우드 워크로드 보안 솔루션 9
- 통합 정책 관리 솔루션 10
- 시큐어 웹 게이트웨이 솔루션 11
- 이메일 보안 솔루션 12
- 엔드포인트 보안 솔루션 13
- 유무선 LAN 인프라 솔루션 14
- SOC 플랫폼 15
- ICS/OT 보안 솔루션 16
- 시큐어 SD-WAN 솔루션 17
- ZTNA 솔루션 18
- Unified SASE 솔루션 19
- 클라우드 네이티브 애플리케이션 보호 플랫폼 20
- 통합 로그 관리 솔루션 21
- 성능 및 보안 침해 공격 시뮬레이션 22
- PAYG 방식의 유연한 라이센스 체계 FortiFlex 23
- 차세대 DLP 솔루션 24
- 이메일(디지털) 워크스페이스 보안 25
- OT 러그드(Rugged) 제품군 26
- OT 사전 예방 보안 전략을 위한 FortiDeceptor 27
- OT 안전한 원격 접속 관리 솔루션 FortiSRA 28

FORTINET

FY 2024 실적

매출
8조 1천억원

거래액
8조 9천억원

2025 1분기 실적

매출
2조 1천억원

거래액
2조 2천억원

운영마진
(GAAP) 29.5%

EPS(GAAP)
$0.56/주

현금 + 투자
6조 6천억원

시가총액
109조원
(AS OF APR. 30, 2025)

고객수

860,000+

누적 출고량

1억 4천만대 이상

지역별 인원

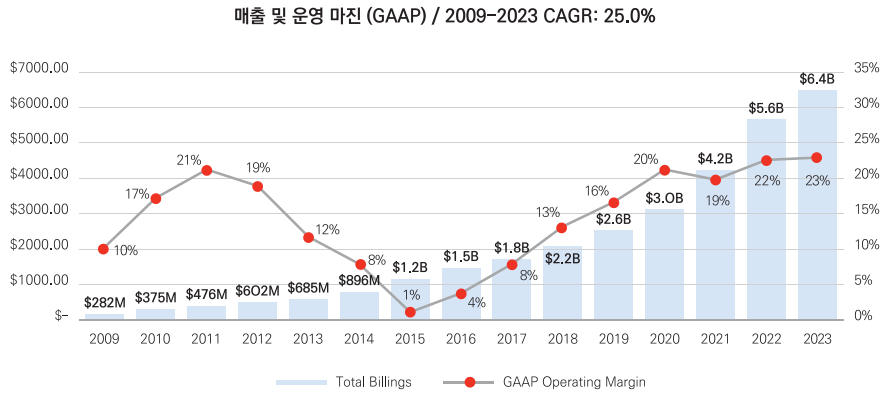
AMERICAS	미국	4,162
	캐나다	2,720
	나머지 미주 지역	1,026
EMEA	프랑스	536
	영국	564
	나머지 유럽, 중동 및 아프리카 지역	2,783
APAC	인도	726
	일본	609
	나머지 아시아 태평양 지역	1,430
총합		14,556

2025년 4월 30일 기준

Securing People, Devices, and Data Everywhere

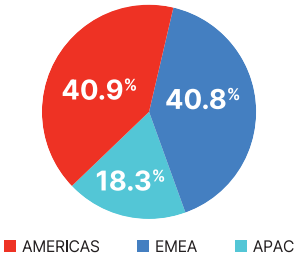
- 설립 연도 : 2000년 8월
- 본사 위치 : 미국 캘리포니아 주
- IPO 시기 : 2009년 11월
- 다우존스 지속가능경영지수(DJSI)에 편입
- 나스닥 100 및 S&P 500 지수 편입

연간 매출 및 수익성을 통한 글로벌 리더

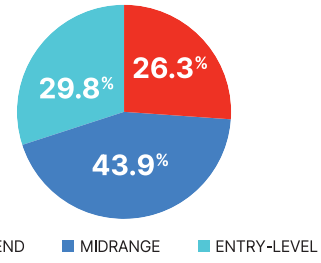


지역 및 세그먼트에 따른 다각화

2025년 1분기
지역별 매출

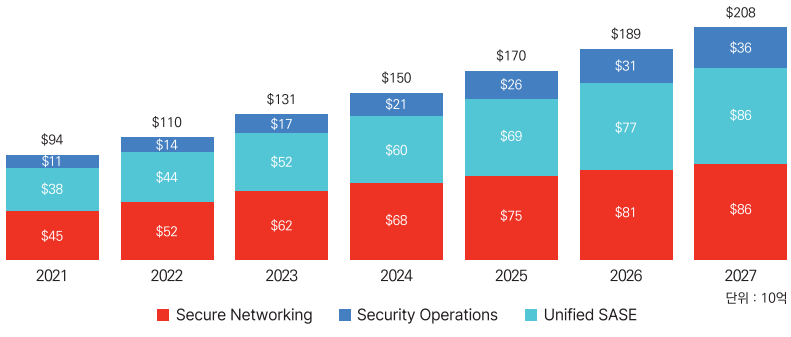


2025년 1분기
세그먼트별 거래액



성장하고 있는 거대한 보안 시장

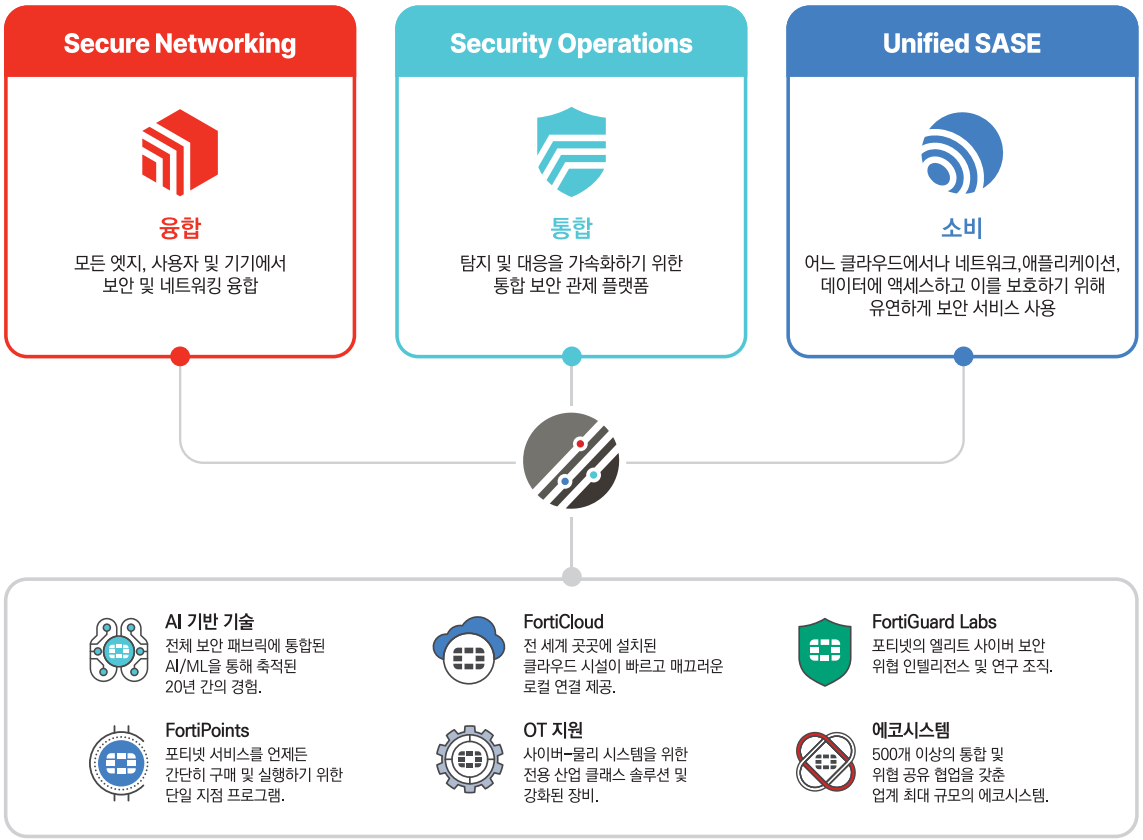
2027년까지 287조원 까지 성장 예정



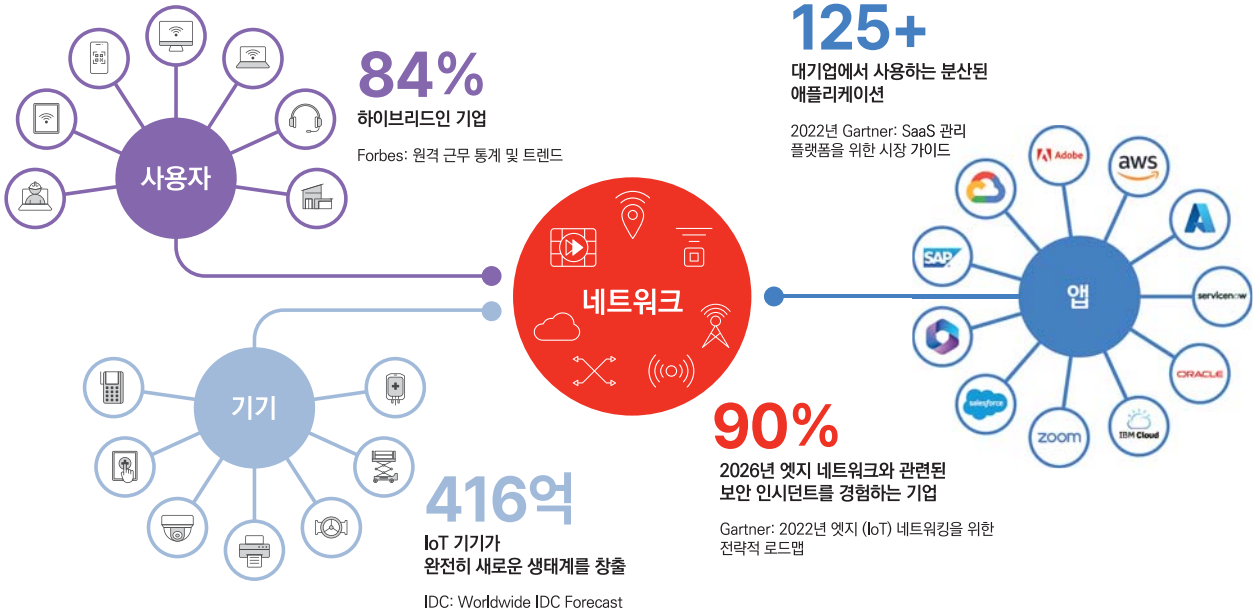
출처: 최근 분석 조사에 따른 포티넷 추정

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

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

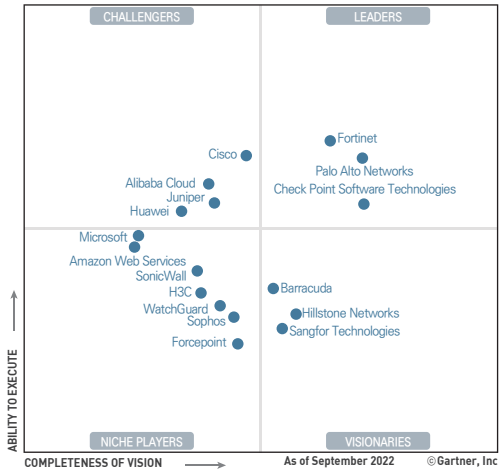
FortiOS를 사용하여 온프레미스, 클라우드, 하이브리드, 융합 IT / OT / IoT 인프라를 포함한 모든 환경에서 일관된 사용자 경험, 공통 보안 정책, 가시성 및 제어를 수행합니다.

SD-WAN 통합기능

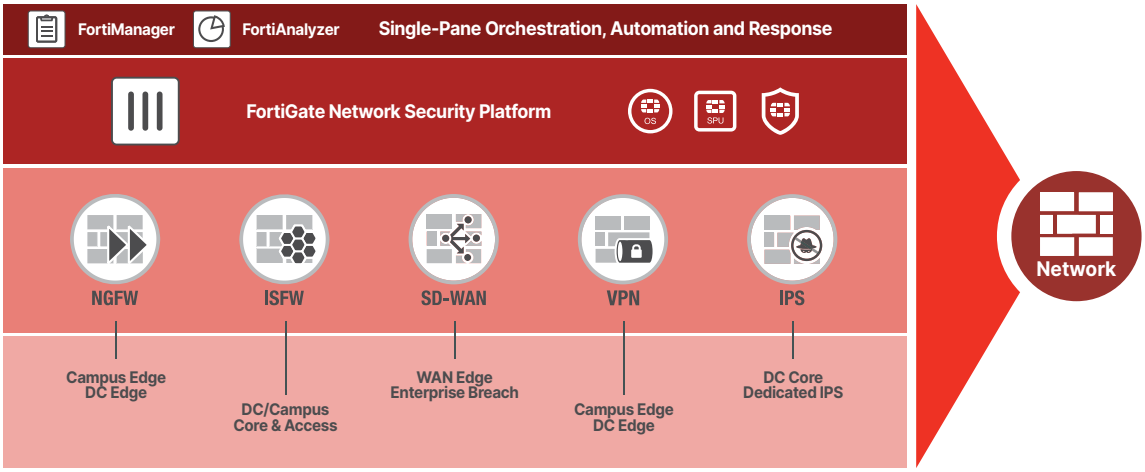
FortiOS 플랫폼을 활용하여 단일 플랫폼에서 SD-WAN 기능을 포함하여 제공합니다. 최신 트렌드인 SASE 관점에서 보더라도, 서비스 에지 기능 및 보안 기능의 통합은 차세대 방화벽의 보안을 더욱 강화해 줍니다.

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.

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.

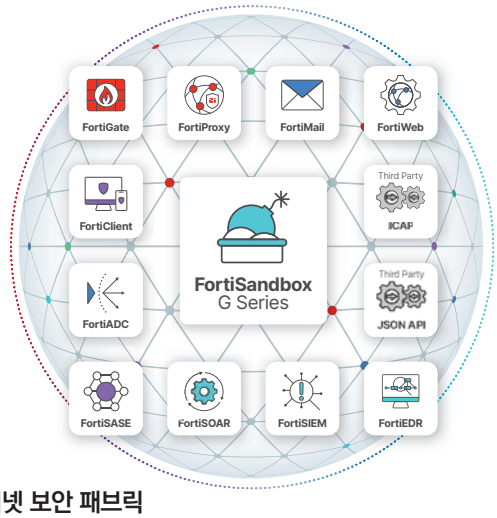
Mitre ATT&CK 기반 보고 및 조사 도구

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.

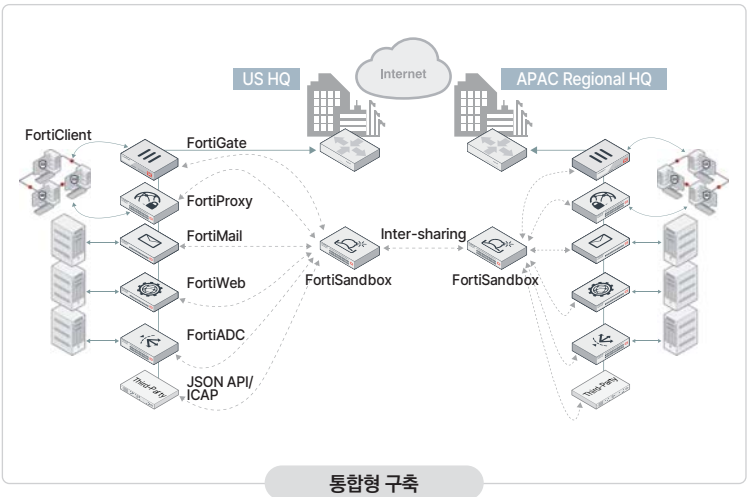
Why FORTINET ?



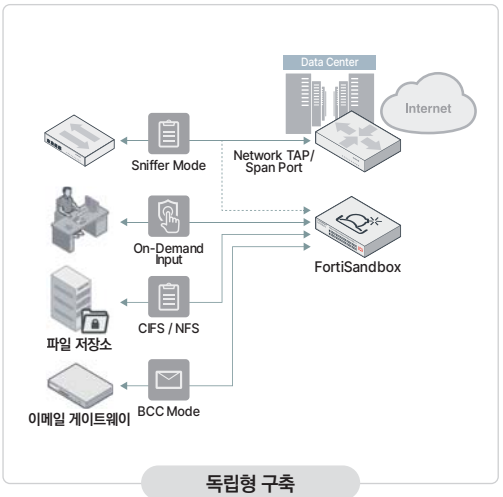
포티넷 보안 패브릭

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.

CASB 솔루션

FortiCASB는 SaaS 애플리케이션에 대한 가시성을 제공하고 동시에 차단 기능을 제공합니다. 사용 중인 SaaS 애플리케이션에 대해서 사용자 기반의 애플리케이션 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.

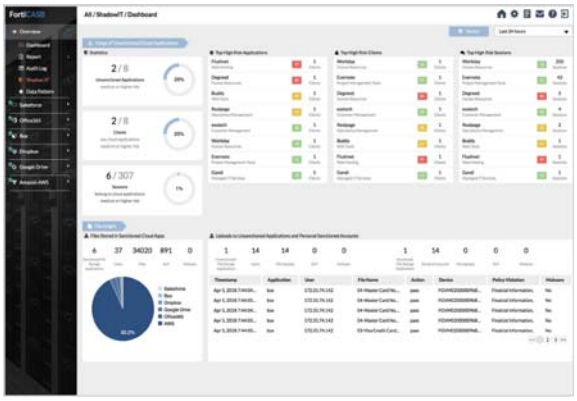
규정 준수 및 DLP

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 애플리케이션 및 SSL 복호화 기능을 포함하여 CASB 기능을 심층적으로 지원합니다.

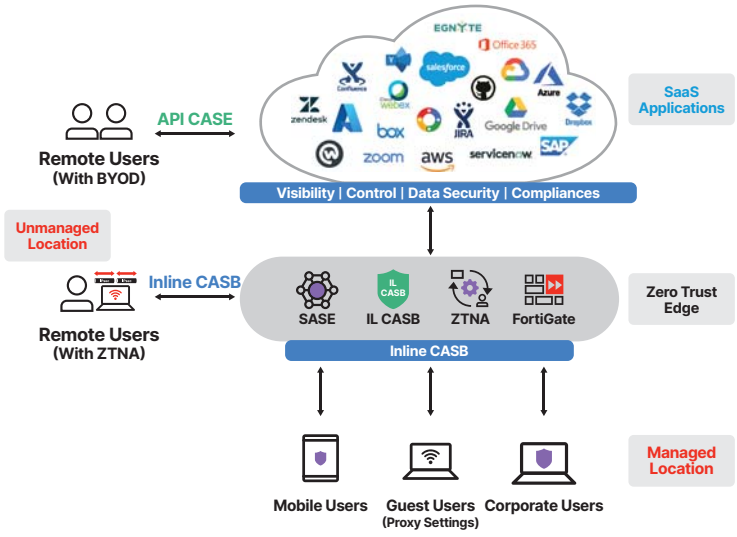
이 솔루션을 어떻게 써야 하나요?

Inline 혹은 API 기반의 구성

포티넷의 ZTNA나 SASE 기술과 인라인으로 직접 연동하거나, SaaS 애플리케이션에 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.



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 ?

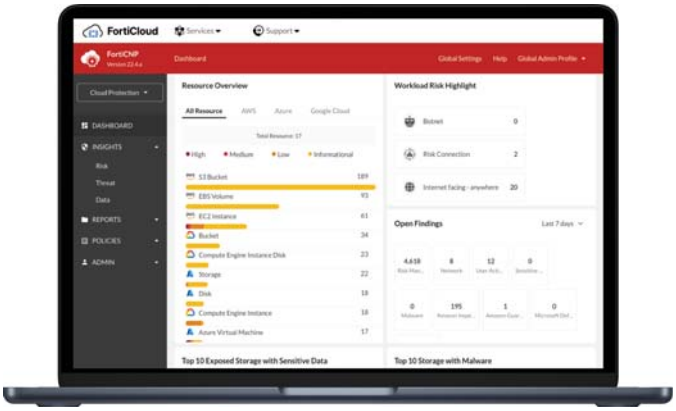
실행 가능한 인사이트를 통한 클라우드 위험 관리

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



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.

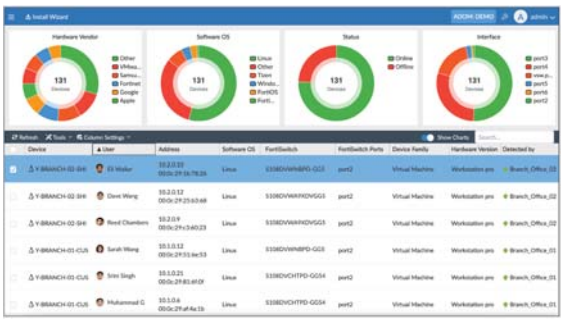
모니터링 및 가시성 문제 해결

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.

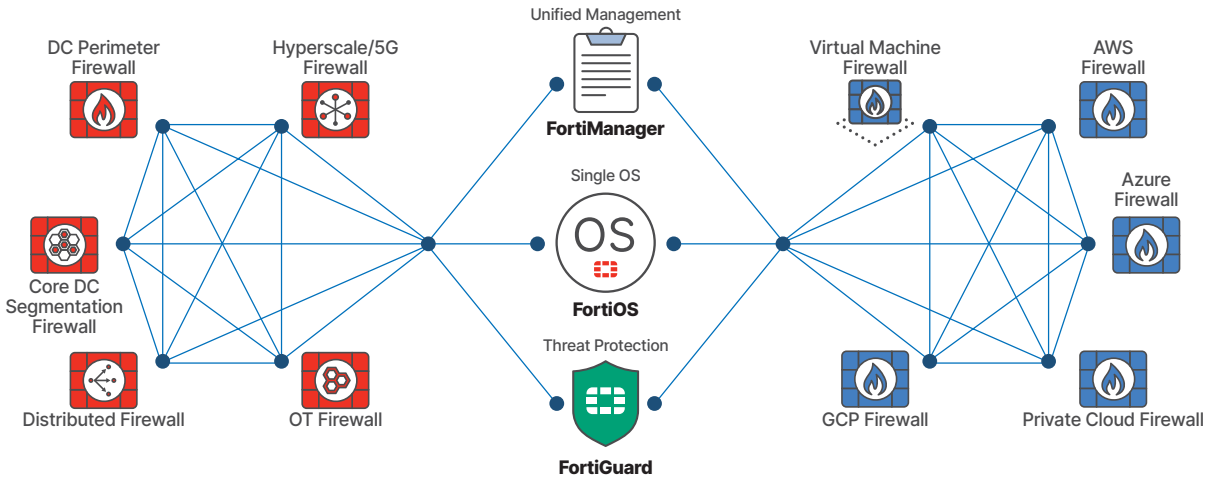
Why FORTINET ?



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.

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.

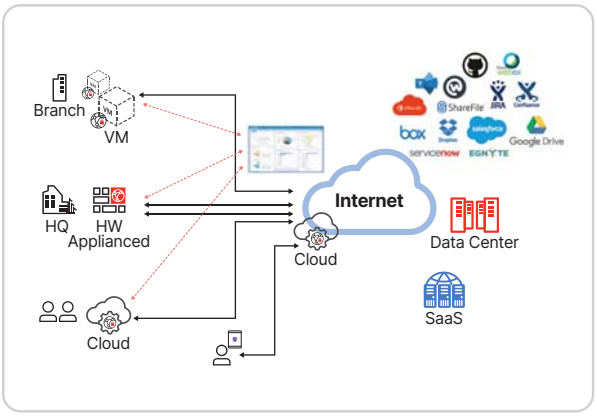
고성능, 확장성 및 낮은 TCO

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.

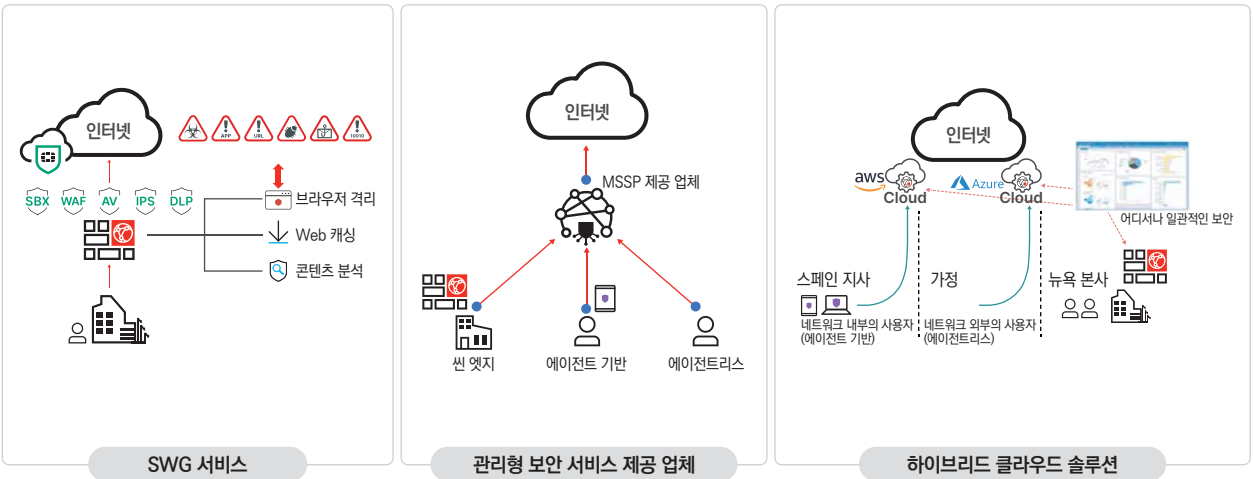
Why FORTINET ?



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.

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

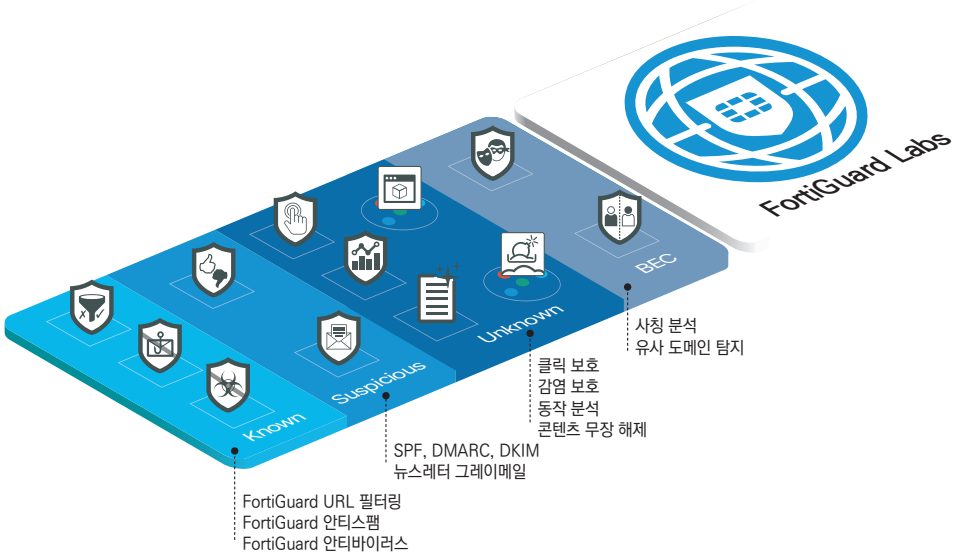
100%
멀웨어 탐지

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.

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 .

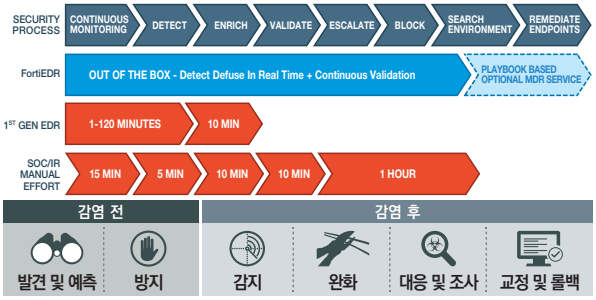
사전 보호

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.

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

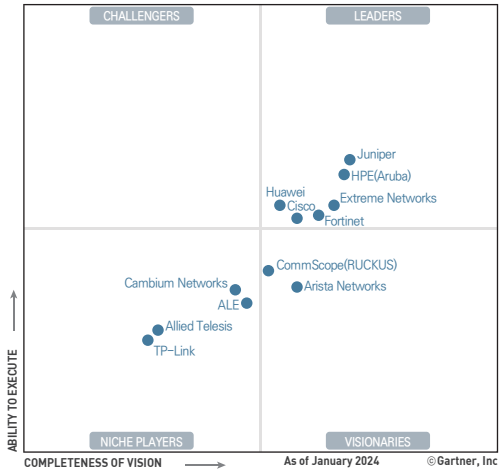
안정적인 NOC와 프로비저닝을 제공하는 포티넷은 하나의 캠퍼스 및 멀티 캠퍼스 환경을 지원하도록 확장할 수 있습니다.

인공 지능(AI)과 머신 러닝(ML)

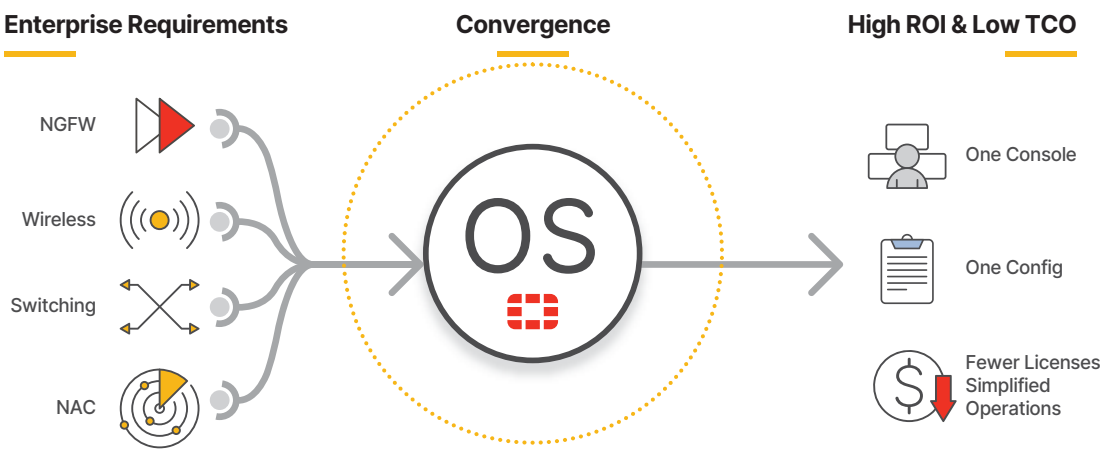
AI 및 ML은 IT팀에게서 반복적인 작업의 부담을 줄여주면서도 트렌드와 네트워크 상태에 대한 알림을 보내 캠퍼스 네트워크를 미리 관리할 수 있도록 합니다.

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.

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.

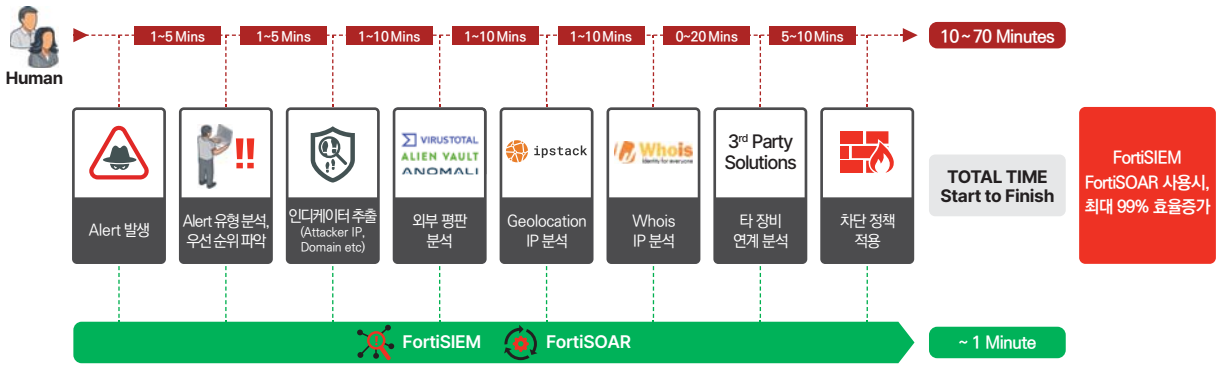
Why FORTINET ?

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

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

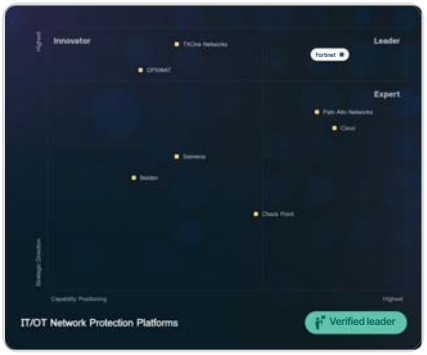
Fortinet의 산업 전문 지식은 석유 및 가스, 운송, 에너지, 전력 및 유틸리티, 제조 등의 산업에서 요구하는 고유한 사이버 보안 요구 사항에 대해 검증된 지원을 제공합니다.

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 ?

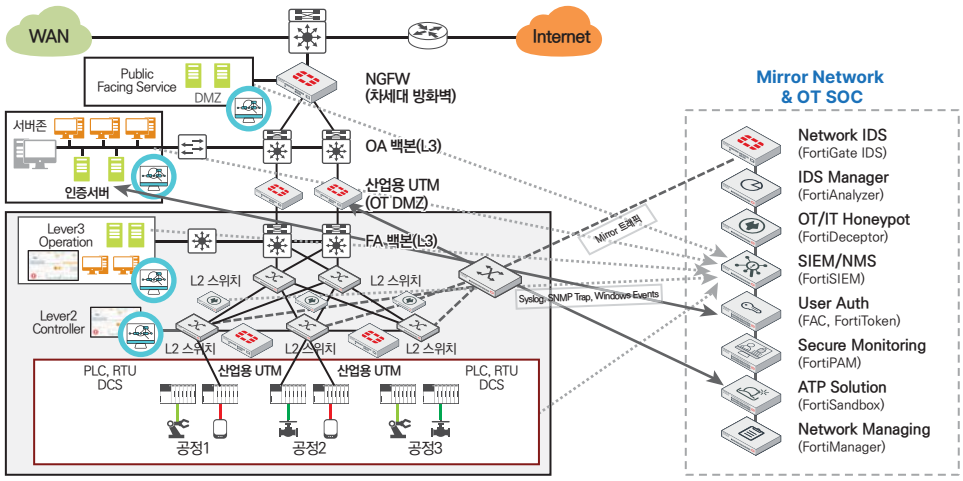
2023 IT/OT Network Protection Platform 분야에서
2년 연속 리더로 선정된 유일한 기업



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.

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

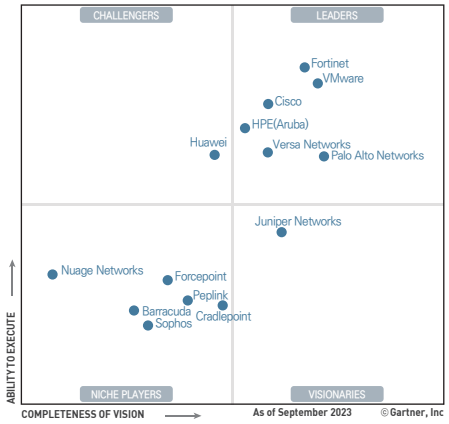
SD-WAN은 중앙 집중식 오케스트레이션, 제로 터치 프로비저닝 및 분석과 더불어 클라우드 온램프의 심층적인 통합을 지원하여 클라우드 연결을 가속화합니다.

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 ?

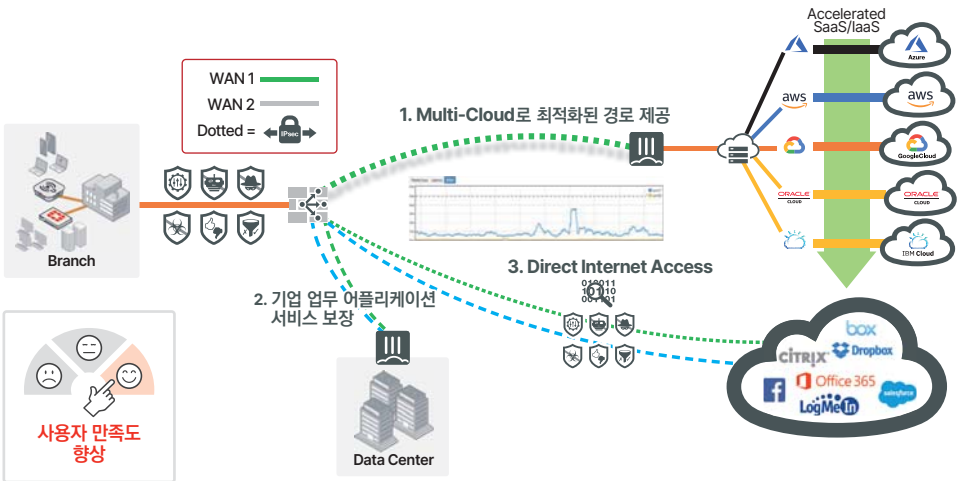
2023년 Gartner® Magic Quadrant™
SD-WAN 부문 Leader로 선정



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.

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 ?

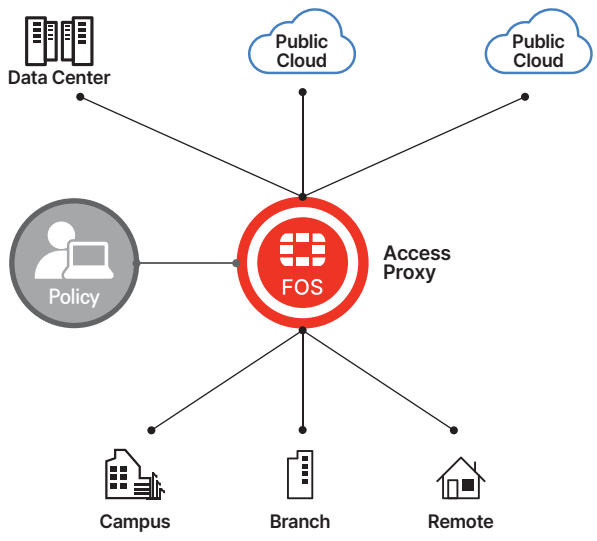
포티넷 ZTNA만의 특징

- 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

Unified SASE 솔루션

클라우드 및 하이브리드 환경의 업무 환경의 모든 사용자와 애플리케이션을 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.

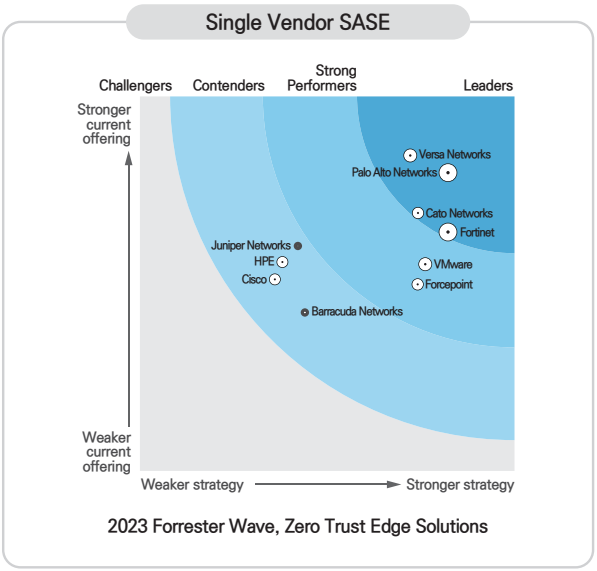
하나의 분석 엔진

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

통합 엔드포인트 에이전트

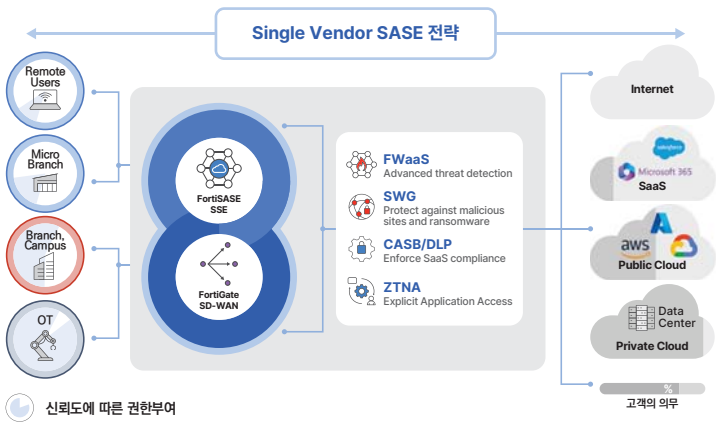
온프레미스, 클라우드를 포함하여 경량화된 통합 엔드포인트 에이전트를 통하여 제로트러스트 환경의 구성이 가능합니다.

Why FORTINET ?



2023 Forrester Wave, Zero Trust Edge Solutions

이 솔루션을 어떻게 써야 하나요?



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

클라우드 네이티브 애플리케이션 보호 플랫폼

FortiCNAPP은 처음부터 code-to-cloud 보안을 위한 통합 플랫폼을 제공하도록 설계되었습니다. 클라우드 네이티브 애플리케이션 라이프사이클의 3단계 (CODE, DEPLOY, RUN) 모두를 위한 모듈을 제공합니다.

솔루션별 특장점

CODE

- 개발 중인 코드 및 API 스캔
- 취약성, 멀웨어 및 잘못된 구성 해결
- 공격 경로 분석으로 위협 우선순위 지정

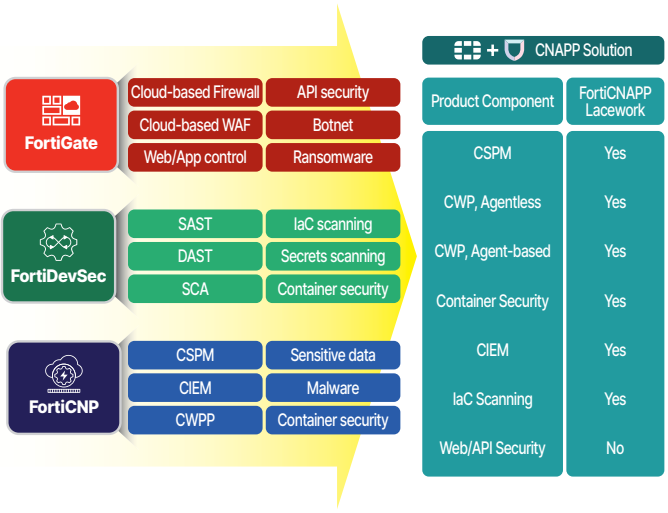
DEPLOY

- 클라우드 인프라 구성 평가
- ID 및 해당 권한 평가
- 규정을 준수하지 않고 취약한 애플리케이션의 배포 방지

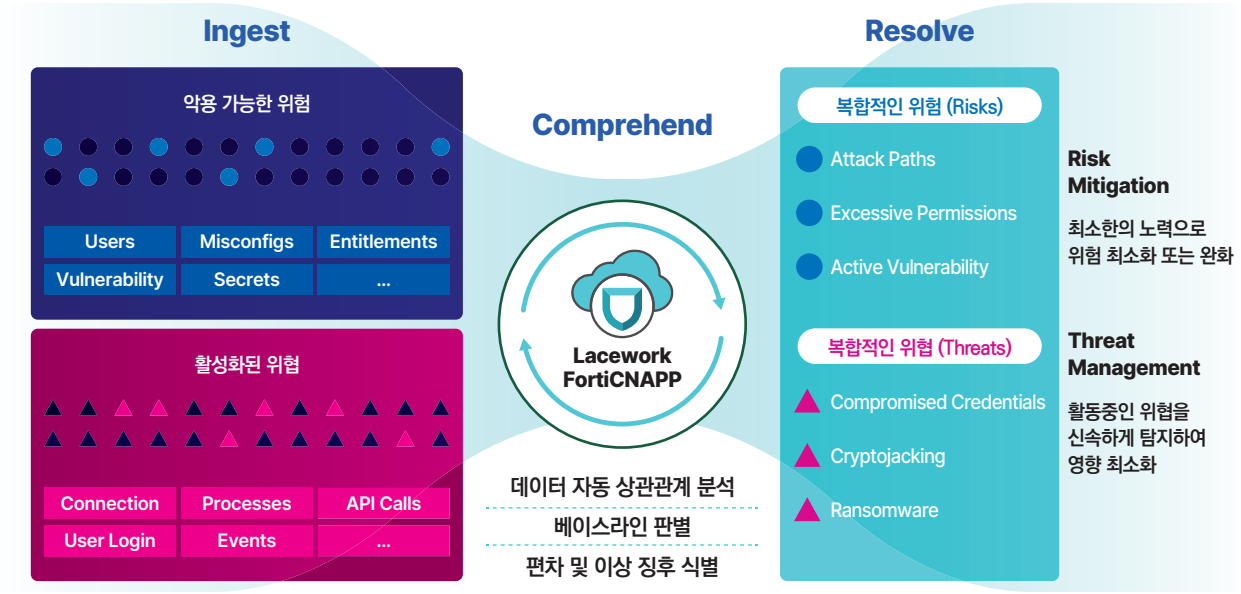
RUN

- 노출되는 민감한 데이터에 대한 지속적인 모니터링
- 비정상적인 행동 및 활성 위협 탐지
- 실행 중인 프로세스 이해 및 네트워크 연결 매핑

Why FORTINET ?



이 솔루션을 어떻게 써야 하나요?



통합 로그 관리 솔루션

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

솔루션별 특장점

통합 가시성

· 기본 보안 패브릭 통합을 통해 하나의 콘솔에서 로그를 집계하고 관리

성능 모니터링 및 AI/ML

· 이상 징후를 찾아내고 위협 환경에 대응 패턴 및 최신 트렌드를 파악

신속한 문제 해결

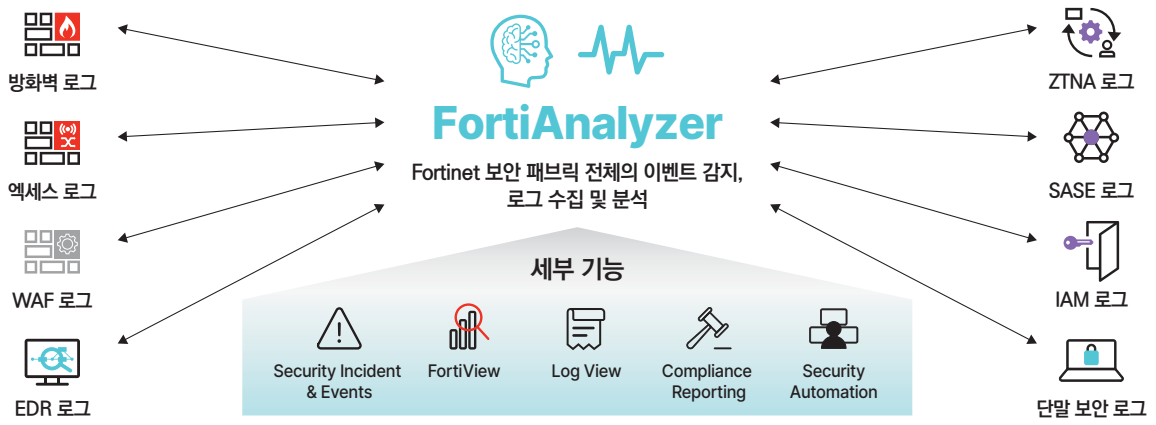
· 자동화된 위협 헌팅, 탐지 및 대응을 통해 신속하게 문제를 해결
· 상관관계분석 및 Playbook 기능을 통한 자동화 기능 제공

유연한 확장 및 연동

· 속도 저하 없는 유연한 확장성 제공
· GenAI나 관리형 보안관제 서비스를 손쉽게 확장

Why FORTINET ?

이 솔루션을 어떻게 써야 하나요?



1 기업 내 이벤트/이슈에 대한 통합 가시성 제공

- FortiAnalyzer는 기업에 로그 관리, 분석, 리포트를 제공하는 강력한 로그 관리 플랫폼
- 단일 콘솔을 통해 Fortinet 장치의 로그를 중앙에서 보고 관리

2 보안, 사용자 정의 이벤트 자동 조치 및 응답

- 중앙 집중화된 Log를 기반으로 이벤트를 정의, 자동으로 동작할 수 있는 자동 조치 기능 제공
- 보안 이벤트, 시스템 이벤트 발생에 대한 조치 시간 단축

3 사전 정의된 다양한 템플릿의 리포트

- FortiAnalyzer에는 즉시 사용 가능한 다양한 보고서가 포함
- 풍부한 리포트 엔진이 포함되어 있어 조직 네트워크 상태에 대한 통찰력 확보

성능 및 보안 침해 공격 시뮬레이션

FortiTester는 기업과 서비스 제공업체가 효과와 성능에 대한 지속적인 검증을 통해 가장 안전한 인프라를 유지할 수 있도록 지원합니다. 네트워크 성능 테스트 및 침해 공격 시뮬레이션(BAS)을 통해 보안과 관련된 인력, 프로세스 및 기술을 평가합니다. FortiTester는 SW번들 및 HW로 제공됩니다.

솔루션별 특장점

보안 솔루션 성능 및 유효성 검증 테스트

IPS, AV등의 시그니처를 포함하여 보안제품의 **ATP 방어 기술**을 확인합니다. (NGFW, FAI, FSA, WAF etc)

Breach 및 성능 시뮬레이션

Throughput, CPS, CCS 등의 TCP/UDP/Application 기반의 Traffic Generation을 수행하거나 MITRE ATT&CK 시뮬레이션도 제공합니다.

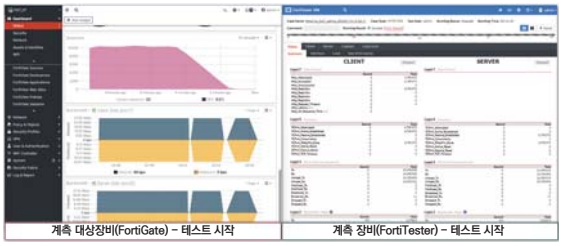
퍼블릭 클라우드 테스트 환경 제공

IaaS, PaaS 등이 제공하는 대로 설계 및 배포된 아키텍처가 예상되는 가용성 및 부하 테스트를 제공하는지 확인합니다.

FortiGuard LABs의 최신 공격 시그니쳐 제공

포티넷의 리서치 기관인 FortiGuard LABs의 글로벌 조직이 전 세계 고객으로부터 올라오는 각종 탐지 정보를 AI 기반으로 분석하여 제공합니다.

Why FORTINET ?



빠르고 간편한 성능 테스트

MITRE ATT&CK 테스트

이 솔루션을 어떻게 써야 하나요?

성능 테스트 (Performance Testing)

- 네트워크 보안장비(방화벽, NGFW 등) 의 성능 요구치를 검증하는 기능
- HTTP, HTTPS, HTTP/2, VPN, DNS, UDP, TCP 등의 CPS, CCS, Throughput 검증의 기능을 제공
- 테스트 후 처리 결과 리포트 제공

보안 테스트 (Security Testing)

- DoS/DDoS 공격 시뮬레이션(Single Packet Flood, TCP/HTTP/CS/UDP Flood)
- Fuzzing 처리능력(잘못된 IP, TCP, UDP, ICMP 패킷 처리능력 검증)
- PCAP Replay / Capture 기능
- IPS/Malware 공격 시뮬레이션

ATT&CK 테스트 (Breach Simulation)

- MITRE ATT&CK 시뮬레이션 제공
- MITRE ATT&CK Framework상 Tactics별, Techniques 공격기술을 사용한 공격 시뮬레이션 제공
- 시뮬레이션 후, 성공/실패여부와 상세 리포트 제공
- Agent 설치 필요

성능테스트와 보안테스트는 Server-Client port 설정으로,
ATT&CK 테스트는 MGMT port와 통신되는 환경에서 테스트 수행

PAYG 방식의 유연한 라이센스 체계 FortiFlex

FortiFlex는 포인트 기반 라이센스 방식을 제공하여 관리자가 보안 서비스 및 지출 규모를 적절하게 조정할 수 있는 유연성과 민첩성을 제공합니다. 포티넷의 사이버 보안 솔루션을 자유롭게 배포하고 동적으로 확장이나 축소가 가능합니다. 포인트가 고갈되더라도 유예기간을 통해 높은 가용성을 유지할 수 있습니다.

솔루션별 특장점

포인트 기반의 라이센스

고객이 유연하고 적정한 사이징을 할 수 있게 되어 비용을 절감할 수 있으며, 계약 기간 내 미사용 포인트는 차년도 포인트 구매시 rollover 되어 함께 사용가능 함.

유연한 확장 및 축소

고객이 일반적인 추가 구매 절차 없이 언제든지 유연하게 Scale up/down/in/out 할 수 있음.

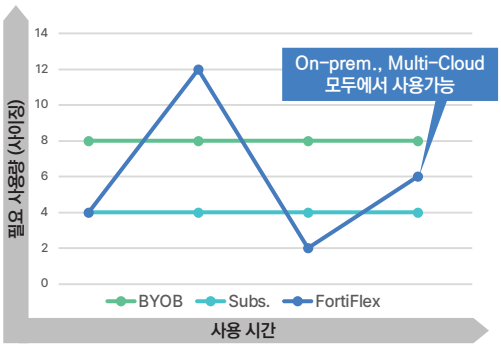
클라우드 포함 멀티플랫폼에 최적화

온프레미스, 클라우드, 멀티클라우드 등 다양한 플랫폼에 사용 가능

통합포털 제공

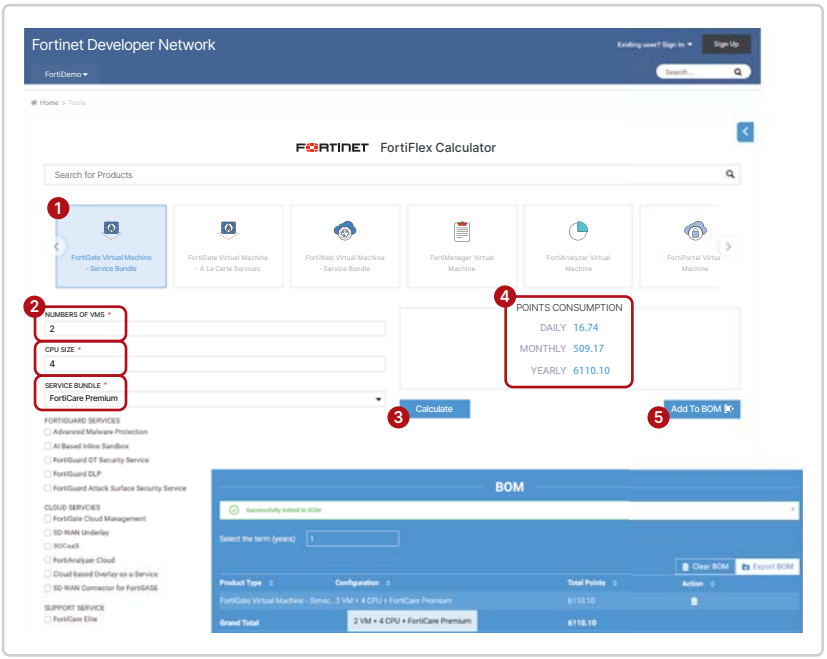
FortiFlex Portal을 통한 라이선스 통합 관리로 가시성 확보 및 운영 효율성 향상

Why FORTINET ?



FortiFlex는 자유로이 사이징 변경 및 다양한 플랫폼(On-premise, Multi-Cloud) 에서 사용 가능 하므로, 즉각적인 확장성 확보와 필요한 만큼의 사용으로 예산 절감 기대 가능.

이 솔루션을 어떻게 써야 하나요?



제품별 소요 포인트 계산 예

1. FortiFlex Calculator 사이트에서 원하는 제품 선택
2. 원하는 사이징 선택
   원하는 서비스 선택
3. Calculate 버튼 누르면
4. 선택한 사이징, 서비스에 대해 일/월/연간 소요 포인트 자동 계산됨
5. Add to BOM (Bill Of Material)

차세대 DLP 솔루션

FortiDLP는 보안 팀이 데이터 유출을 예측 및 방지하고, 내부자 위험을 탐지하며, 직원에게 적절한 사이버 보안 교육을 실시할 수 있도록 지원하는 차세대 클라우드 네이티브 엔드포인트 데이터 보호 솔루션입니다. 경쟁 솔루션과 달리 FortiDLP는 데이터 손실 방지, 내부자 위험 관리, SaaS 데이터 보안, 위험 정보에 기반한 사용자 교육을 결합하여 데이터 보호에 대한 통합된 접근 방식을 제공합니다.

솔루션별 특장점

강력한 가시성

클라우드, 시스템, 사용자, 데이터 및 네트워크에 대한 원격 분석을 통해 강력한 가시성을 제공하며, 조직의 원본 데이터를 보호합니다.

빠른 대처 시간

정책 없이도 적용 가능한 엔드포인트 및 클라우드 센서를 통해 빠르게 가시성을 확보

다양한 환경 지원

관리형 및 비관리형 디바이스에서 수신부터 송신까지 동적 응답으로 데이터를 보호

분석 가속화

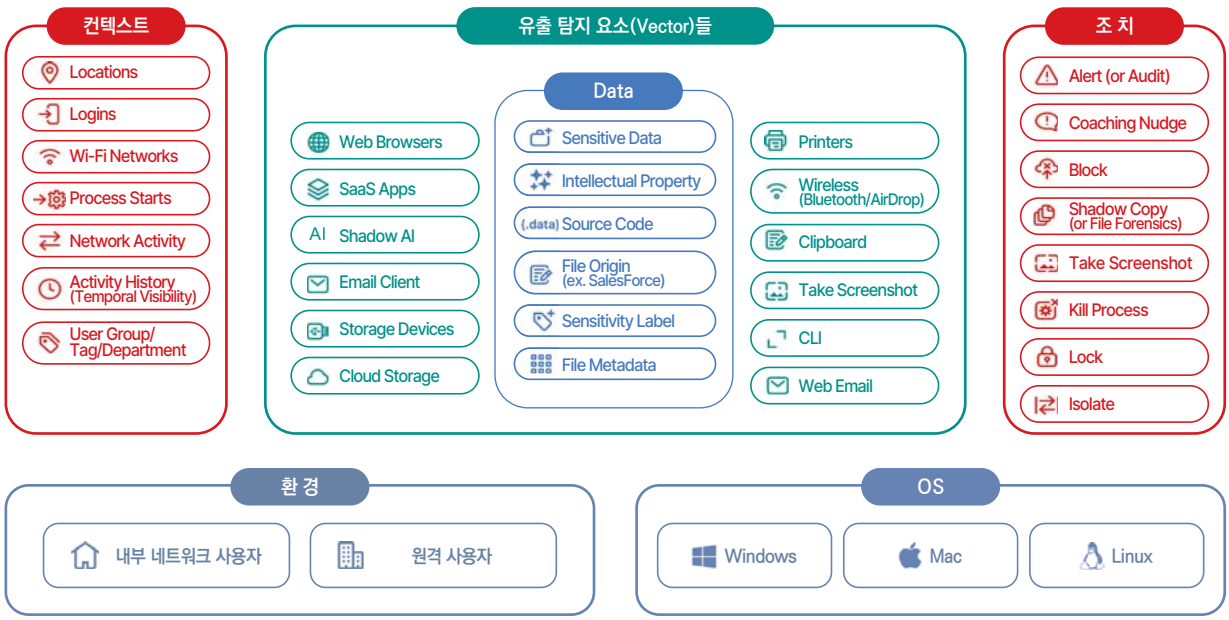
AI로 강화된 내부 위협 활동 탐지와 차단 및 대응 시간을 단축하는 워크플로, FortiAI(AI 어시스턴트)를 활용한 나만의 LLM 구축

Why FORTINET ?

전방위적인 DLP플랫폼

데이터 도난을 예측하고 방지하는 차세대 엔드포인트 DLP 및 내부자 위협 관리에 매우 효과적입니다.

이 솔루션을 어떻게 써야 하나요?



이메일(디지털) 워크스페이스 보안

이메일을 포함한 현재의 디지털 워크스페이스 환경의 변화는 보안의 측면에서도 새로운 접근이 필요하게 되었습니다. 단순 이메일 뿐 아니라 클라우드 상의 다양한 협업툴로 소통의 공간이 확장 되었기 때문 입니다. FortiMail Workspace는 클라우드 환경에 특화되어 있습니다. M365, Google WorkSpace, Exchange등의 클라우드 혹은 이메일 서비스 뿐 아니라 SharePoint, Teams, OneDrive, Slack, AWS S3, Box 등을 포함하는 통합 솔루션을 제공 합니다.

솔루션별 특장점

정적 및 동적 분석 엔진

다단계의 정적 엔진과 실시간에 가까운 동적 분석 엔진을 통해서 위협이 서비스를 사용하는 조직에 도달하기 전에 이를 방지합니다.

AI 기반 피싱 및 BEC 차단 기술

자연어 처리와 AI를 활용해 텍스트 내 감정 표현과 클릭 유도 문구를 분석하고, 악의적인지 여부를 판단합니다.

SaaS 앱 보안

API를 통해 손쉽게 배포되는 클라우드 네이티브 플랫폼은 이메일, 브라우저, 협업 채널, 스토리지 솔루션 등에 대한 보안을 통합합니다.

기본제공 되는 관리형 IR 서비스

인시던트에 대한 모니터링, 분석, 온디맨드 조사 및 보고서를 작성해 줍니다. 보이지 않는 새로운 공격과 능동적 Threat Hunting을 지원 합니다.

Why FORTINET ?

99.95% 탐지
100% 빈틈없이 검사
75% SOC 예산 절감

이 솔루션을 어떻게 써야 하나요?

사용자 작업 공간 전반으로 보안을 확장하여 이메일, 웹, Slack 및 Teams와 같은
협업 애플리케이션과 클라우드 스토리지 앱을 보호합니다.

OT 러그드(Rugged) 제품군

포티넷 러그드 제품군은 NGFW를 포함한 다양한 제품 라인업을 보유하고 있으며 극한의 환경에서도 시스템을 연결하고 보호하는 데 필요한 내구성과 저항력을 갖춘 특수 제작된 어플라이언스입니다. 방화벽, 스위치, AP 등 다양한 프로토콜과 표준을 준수하여 OT 네트워크에 단순하고 고성능의 솔루션을 제공하는 동시에 TCO를 절감합니다.

솔루션별 특장점

OT 컴플라이언스 대응

자동화, 오케스트레이션 및 규정 준수를 위한 통합 보안 플랫폼

Rugged NGFW

포티게이트 러그드 시리즈 차세대 방화벽(NGFW)은 네트워크 의 전체 성능에 영향을 최소화 하면서 강력한 네트워크 보안 환경을 구현해 줍니다.

Rugged Switch

FortiSwitch™ 러그드 스위치는 신뢰할 수 있는 스위치 환경의 모든 엔터프라이즈 기능, 성능, 보안을 제공합니다. 특히 열악한 환경뿐 아니라 OT 산업 및 제어 네트워크에도 적합합니다.

Rugged AP

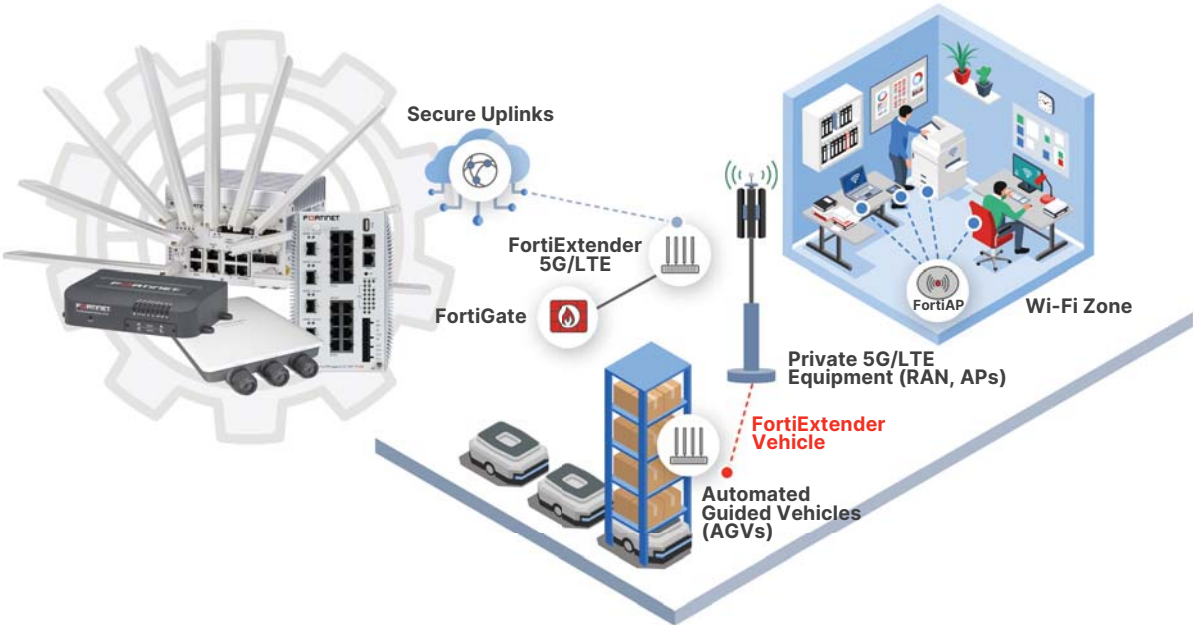
FortiAP 러그드 AP는 열악한 환경에서 안정적인 무선 환경을 제공 합니다. 특히 무선 통합 컨트럴러가 FortiGate에 내장 되어있기 때문에 유무선 복합네트워크에 최적의 보안을 제공합니다.

Why FORTINET ?

포티넷, 2023 IT/OT 네트워크 보호 플랫폼 내비게이터™에서 단독 리더로 선정

reddot winner 2024

이 솔루션을 어떻게 써야 하나요?



OT 사전 예방 보안 전략을 위한 FortiDeceptor

포티넷 SecOps 플랫폼의 일부인 FortiDeceptor는 인증정보 도용, 내부 확산, 중간자 공격, 랜섬웨어와 같은 네트워크 내 공격을 탐지하고 대응합니다. 사이버 보안 전략의 일부로 FortiDeceptor를 추가하면 침입 기반 탐지와 상황별 인텔리전스를 결합하여 방어를 사후 대응에서 사전 예방으로 전환하는 데 도움이 됩니다.

솔루션별 특장점

OT/IOT/IT

- 패시브 풋프린트를 통한 네트워크 가시성 및 침해 탐지
- 자체 원격 분석을 제공할 수 없는 자산에 대한 위협 탐지

제로데이 익스플로잇 식별

- 디코이는 이전에 알려지지 않은 취약점을 드러내어 즉각적인 조사가 가능한 조기 경고를 제공합니다.
- 멀웨어가 '실제' 데이터를 암호화하고 확산되는 것을 방지합니다.

레터럴 무브먼트

- 네트워크를 탐색하려는 공격자를 미끼 자산으로 유도하여 공격자의 움직임을 실시간으로 모니터링할 수 있습니다.
- 최후의 수단인 보안 제어("다른 모든 제어가 실패했을 때 탐지")

침해 후 탐지

- 속임수 미끼를 활용하여 공격 발원지 추적
- 고도로 모니터링되는 환경에서 공격자를 관찰하여 공격자 TTP에 대해 학습합니다.

Why FORTINET ?

공격자를 가짜 자산인 디지털 고스트로 유인하여
기업의 실제 자산을 보호

이 솔루션을 어떻게 써야 하나요?

1 검색 / 분석

고객사 환경을 분석하여 내부자 위협, 또는 외부 공격자의 ATP로부터 알맞은 Decoy를 배포할 수 있도록 분석합니다.

여기에서 Asset Discovery 기능을 추가로 활용할 수 있습니다.

2 배포

고객사 환경에 맞게끔 Decoy와 Lure를 적절히 배포합니다.

디셉터 계층을 실제 IT자산이 포함된 범위로 지정하여 자동 Decoy 배포 기능 사용이 가능합니다.

3 탐지

내부자 또는 외부 공격자가 Decoy(유인시스템)에 접근하도록 유도합니다.

앞서 언급한 Breadcrumbs와 가짜 비커닝 트래픽으로 시스템이 자동적으로 유인할 수 있습니다.

4 대응

공격자 IP의 자동 검역, 고객사 환경만의 실행 가능한 인텔리전스 획득

FortiDeceptor를 통해 공격자들이 발굴한 잠재된 위협, 공격 방법 등을 확인하고 즉각적인 대응을 수행합니다. 또한 중앙 모니터링 및 자동화 대응을 위해 "any"SIEM 또는 SOAR와 연동할 수 있습니다.

여기에서 Mitre Att&CK For ICS Dashboard 기능을 추가로 활용할 수 있습니다.

수동적이지만 포괄적인 위협 탐지를 통해 보안 가시성 격차를 줄이고,
공격자가 민감한 자산에 접근하는 것을 디셉션 시스템으로 유도하여 공방의 균형을 방어자의 이점으로 전환

OT 안전한 원격 접속 관리 솔루션 FortiSRA

신뢰할 수 있는 네트워크에 신뢰할 수 없는 네트워크의 사용자가 접속하려고 할 때 FortiSRA를 통과하는데, FortiSRA는 안전한 원격 액세스, 자격 증명 관리, 라이브 세션 모니터링 및 기록, 안전한 파일 전송 및 데이터 유출 방지 기능을 제공합니다. FortiSRA는 엔드포인트 에이전트가 필요하지 않으므로 관리자가 SCADA, DCS, IACS를 포함한 OT 시스템에 대한 직원 및 타사 원격 액세스를 보호할 수 있습니다.

솔루션별 특장점

Agent-Less

다양한 범용 프로토콜을 사용한 다양한 작업을 웹 브라우저를 통해 안전하게 수행할 수 있도록 설계되었습니다.

감사증적 및 접근제어

사용자 작업 시작/종료 시 체크인, 체크아웃 강제 할당, 작업시간 설정, 명시적 접속 승인 등의 다양한 타겟 시스템 보호 기능들을 제공 합니다.

녹화 및 차단 기능

사용자 작업 녹화 조회와 실시간 모니터링, 작업 세션 차단을 통한 강력한 작업 감시 기능을 제공 합니다.

FortiGuard 글로벌 인텔리전스 활용

사용자 파일 업로드 및 다운로드의 악성코드를 탐지하고 차단하는 Antivirus 검사 기능과 문서 유출을 탐지하고 차단하는 DLP 기능이 탑재 되어 있습니다.

Why FORTINET ?

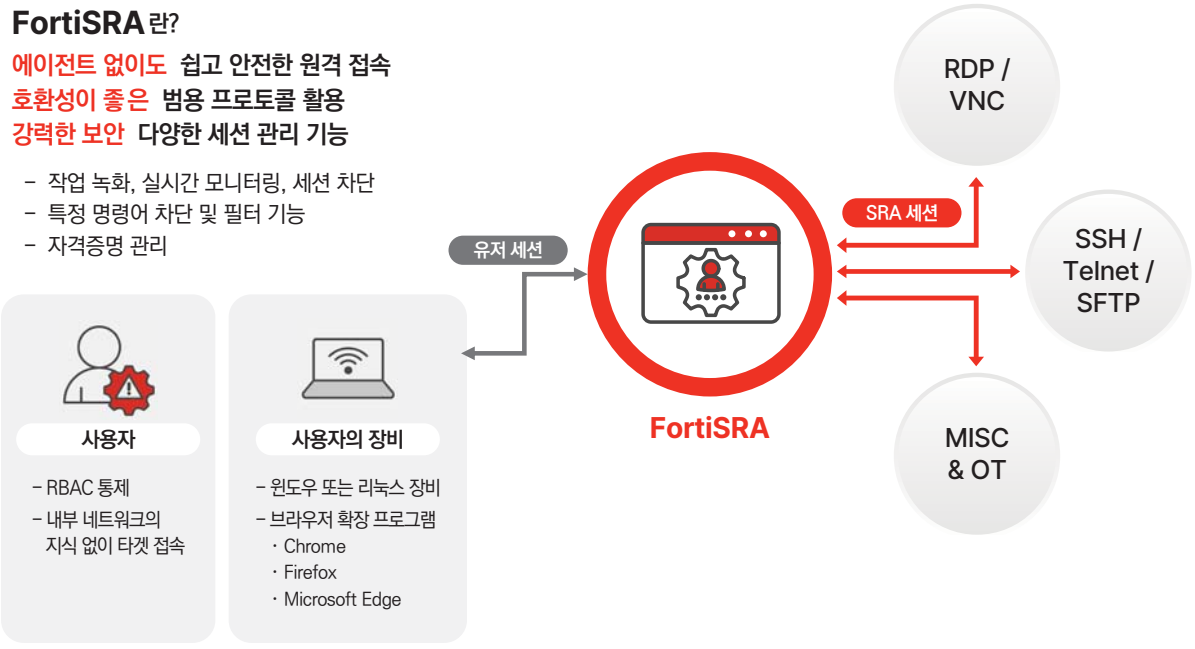
- 원격 사이트 운영 및 관리 (O&M)
- 시스템 상태 모니터링 유지보수 및 진단 (M&D)
- 시스템 시운전 (FAT/SAT)
- 로그 및 기록 검색 결함 분석 및 문제 해결

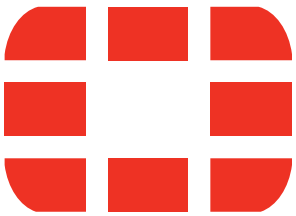
이 솔루션을 어떻게 써야 하나요?

FortiSRA 란?

에이전트 없이도 쉽고 안전한 원격 접속
호환성이 좋은 범용 프로토콜 활용
강력한 보안 다양한 세션 관리 기능

- 작업 녹화, 실시간 모니터링, 세션 차단
- 특정 명령어 차단 및 필터 기능
- 자격증명 관리





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