FortiGate 소개자료

Fortinet Korea SE Team

FY2025 Q1

포티넷 코리아 주력 솔루션과 제품

Secure Networking

보안과 네트워킹을 통합하여 모든 에지와 장치를 보호

1. 엔터프라이즈 방화벽
가트너가 평가한 업계 최고의 차세대 방화벽

2. 보안 스위치
우수한 가시성과 NAC 기술을 내장한 매니지드 보안, 고성능 보안 스위치

2. 무선 AP
우수한 무선 품질과 가시성, 사용자별 무선 접속 솔루션

3. Rugged 제품 - OT보안
OT 등 혹독한 환경에서도 사용할 수 있는 Rugged 타입의 방화벽, 스위치, AP, 디셉터 등

4. FG/FortiLAN 클라우드
SaaS 형태로 제공되는 다양한 포티넷 제품에 대한 원격 관리 서비스

5. 통합 정책 관리 매니저
포티넷 제품 대상의 중앙 집중형 보안 정책 관리 및 프로비저닝 솔루션

6. AIOps
AI와 ML 기술을 이용한 포티넷 유무선 서비스 및 SD-WAN 네트워크 품질 관리 솔루션

7. 사용자 인증 관리
중앙 인증 관리 솔루션 (MFA, 로컬, AD / LDAP 연동, Radius 인증, SAML)

8. 2FA 토큰
일회성 비밀번호 생성 및 푸쉬 알림 솔루션

9. 트래픽 시뮬레이터
성능 시험 및 보안 테스팅 (BAS, Breach Attack Simulation) 솔루션

10. 개발자 FNDN
포티넷 제품 API 개발 정보와 툴을 제공하는 유료 개발자 커뮤니티 서비스

11. 포티가드 시큐리티 서비스에서 제공하는 시그니처 업데이트 서비스

- IPS 침입 탐지 방지
- AV 안티 바이러스 (악성코드 방지)
- 웹 URL 데이터베이스
- 안티 봇넷, C&C
- Geo IP 위치 정보
- 웹 방화벽 룰
- 클라우드 / 온-프레미스 샌드박스
- OT 산업용 프로토콜 분석
- IoT 사물인터넷 기기 탐지

Unified SASE

어디서나 사용자와 기기와 애플리케이션을 보호

12. SASE
원격 근무지 및 사용자의 접속 위치에 상관없이 사이버 공격으로부터 뛰어난 보호를 제공하는 클라우드 보안 솔루션

13. 제로 트러스트 네트워크 접속 보안 ZTNA
원격 접속 제어, 애플리케이션 접속 정책과 단말기 리스크 제거를 위한 제로 트러스트 엔드포인트

14. FortiClient - 패브릭 에이전트
엔드포인트 단말기 정보, IPSec / SSL VPN 접속 에이전트

15. 시큐어 SD-WAN 솔루션
애플리케이션 기반의 NGFW 보안과 SD (Software Defined)-WAN 통합 솔루션

16. 디지털 서비스 품질 모니터링 (DEM)
클라우드 워크로드 서비스와 온-프레미스 인프라의 성능 저하 및 장애 상태 모니터링 솔루션

17. 시큐어 웹 게이트웨이
URL 프록시 서비스, 클라우드 워크로드에 대한 테넌트별 접속 제어 등의 애플리케이션 통제 솔루션

18. 원격 브라우저 격리, RBI
웹 브라우저를 통한 악성코드 유입 차단하는 ATP 솔루션

19. 방화벽 가상머신, FG-VM
퍼블릭 클라우드와 프라이빗 클라우드 워크로드 보호를 위한 가상머신 VM 방화벽

20. 웹 방화벽, API 보안
OWASP 및 웹 API 애플리케이션 공격 탐지 및 방어 솔루션

21. 클라우드 네이티브 방화벽 CNF for AWS
클라우드 네이티브, AWS 방화벽 매니저 서비스와 연동 지원하는 포티게이트 NGFW 방화벽, IPS 솔루션

22. CASB
SaaS 애플리케이션 설정 오류로 인한 보안 홀과 데이터 유출 그리고 컴플라이언스 준수 여부 검사를 위한 SaaS 서비스

Security Operations

AI 기반 보안 운영으로 대규모 위협을 탐지, 조사 및 대응

23. 샌드박스
알려지지 않은 악성코드 탐지용 샌드박스 솔루션

24. 이메일 보안 게이트웨이
시큐어 이메일 서버 및 게이트웨이를 통한 이메일 보안 솔루션

25. EndPoint 탐지 및 대응, EDR
자동화된 엔드포인트 보호 및 인시던트 대응 관리 솔루션

26. 악성코드 NDR
AI와 ML기술을 이용한 대용량 초고속 악성코드 탐지 솔루션

27. 접근 관리 솔루션, PAM
OT 인프라 환경과 같은 보안수준이 높은 시스템 접속 사용자 접근 권한 관리 시스템

28. 사이버 디셉션
허니팟 한계를 넘어선 액티브한 보안 침입 탐지용 디셉션 솔루션

29. 피싱 메일 시뮬레이션
실제 피싱 기술 기반으로 직원들에 대한 피싱 테스트

30. 통합 로그 관리 솔루션
포티넷 제품 보안 로그 연관 관계 분석, 리포트 및 저장 관리 솔루션

31. 보안 정보 및 이벤트 관리, SIEM
SIM(보안 정보 관리)과 SEM(보안 이벤트 관리) 솔루션

32. 보안 오케스트레이션, 자동화 및 대응, SOAR
IT 인프라 보안 업무 프로세스 자동화 솔루션

33. 디지털 리스크 보호 서비스, DRPS
기업의 브랜드 리스크 관리, 자산 및 데이터 보호 솔루션

34. 클라우드 네이티브 프로텍션 CNP
멀티-클라우드 워크로드의 보안 위협과 컴플라이언스 준수 여부를 통합 관리 솔루션

35. 동적 어플리케이션 보안 테스트, DAST
웹 애플리케이션의 동적 보안 테스트를 수행하여 공격자가 악용할 수 있는 취약성을 식별

네트워크 및 보안 트렌드

글로벌 고객사들의 트렌드

Top Strategic Technology Trends for 2022: Cybersecurity Mesh

Accelerating Growth	Sculpting Change	Engineering Trust
• Generative AI	• AI Engineering	• Cloud-Native Platforms
• Autonomic Systems	• Hyperautomation	• Privacy-Enhancing Computation
• Total Experience	• Decision Intelligence	• **Cybersecurity Mesh**
• Distributed Enterprise	• Composable Applications	• Data Fabric

Source: Gartner

매년 IT 동향에 대한 연례 보고서를 발표하는 **가트너**는 **2022년**의 **[전략 기술 트렌드 Top 12]**를 소개 했습니다.

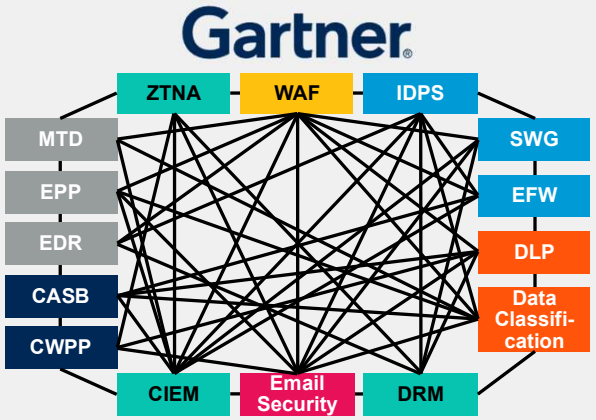
가트너는 전략적 IT 동향에 대한 연례 보고서를 통해 **AI와 클라우드, 보안** 또는 **엔지니어링에 대한 디지털 투자** 등 12개의 사항이 오는 **2022년 최고의 기술 추진 요인**이 될 것으로 전망했습니다.

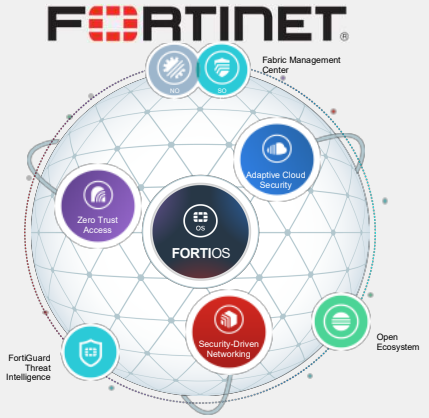
그 중에서 **사이버 보안 메쉬**에 대해 언급하며 이는 새로운 트랜드이며, 2022년 및 가까운 미래에 대한 가트너의 **최고 전략 기술 동향**이 될 것으로 이야기했습니다. **사이버 보안 메쉬**는 기업이 분산된, 가장 필요한 인프라 등에 보안을 배포 및 확장할 수 있도록 하는 보안 아키텍처에 대한 **현대적인 접근 방식**으로, 더 큰 확장성, 유연성 및 안정적인 사이버 보안 제어를 가능하게 합니다.

가트너는 증가하는 사이버 보안 위협은 보안 기술의 혁신을 불러일으키고 있으며 **2024년까지 CSMA를 채택하는 조직이 개별 보안 침해 사고로 인한 발생할 수 있는 재정적 피해를 평균 90% 감소시킬 수 있다고 이야기 하였습니다.**

포티넷 시큐리티 패브릭 소개

사이버 보안 메쉬 아키텍처에 부합하는 포티넷 제품





Gartner는 “2024년까지, 사이버 보안 메시 아키텍처를 채택하여 여러 보안 도구를 통합해 협업 에코시스템 형태로 운영하는 기업은 개별적인 보안 침해사고가 미치는 경제적 손실을 평균 90%까지 줄일 수 있을 것” 이라고 전망합니다.

“Top Strategic Technology Trends for 2022: Cybersecurity Mesh, Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi, 18 October 2021”

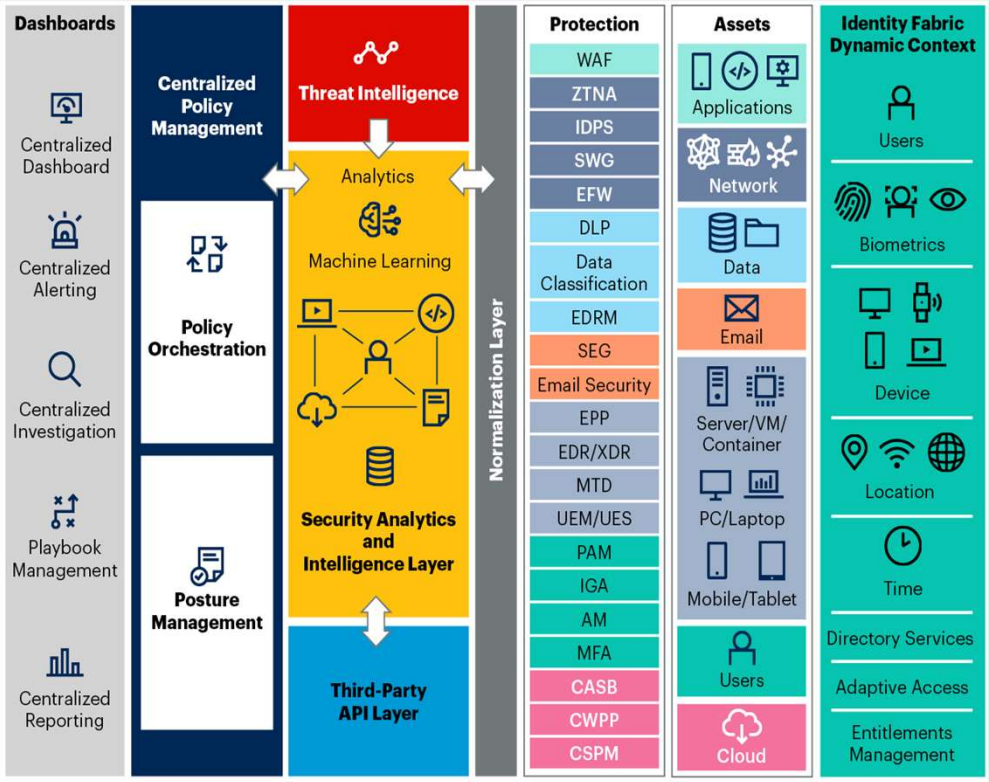
Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi. As of October 2021

사이버 시큐리티 메쉬 아키텍처 (CSMA) 구축 목표에 부합하는 포티넷 시큐리티 패브릭 기술

- 모든 엣지를 커버하는 높은 **가시성** 제공
- 분산된 보안 솔루션을 **중앙 원격 관리** 지원
- 하이브리드 환경에서 **일관된 보안 정책 적용** 지원
- 포티넷 시큐리티 패브릭 솔루션의 실시간 글로벌 **위협 인텔리전스** 정보 연동 지원
- 보안 조치 대응 **자동화** 툴 & **API** 지원
- 광범위한 대상 장비 지원, 최적화된 연동 기능 지원하는 **오픈 에코 파트너** 환경 지원

포티넷 시큐리티 패브릭 소개

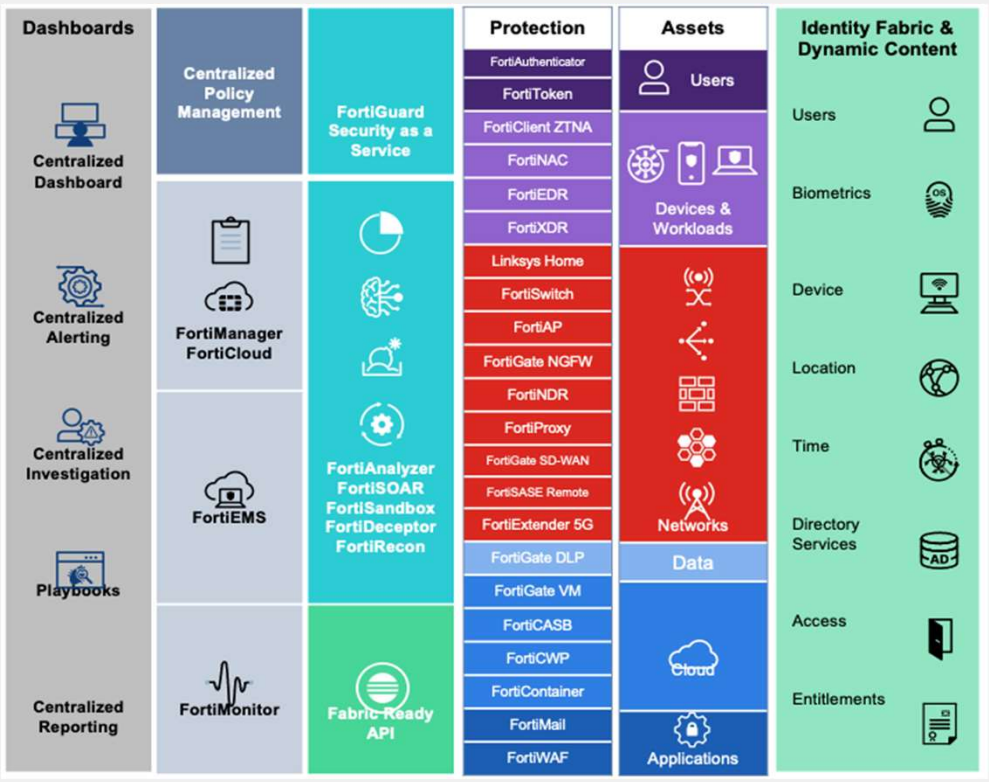
Gartner



Source: Gartner

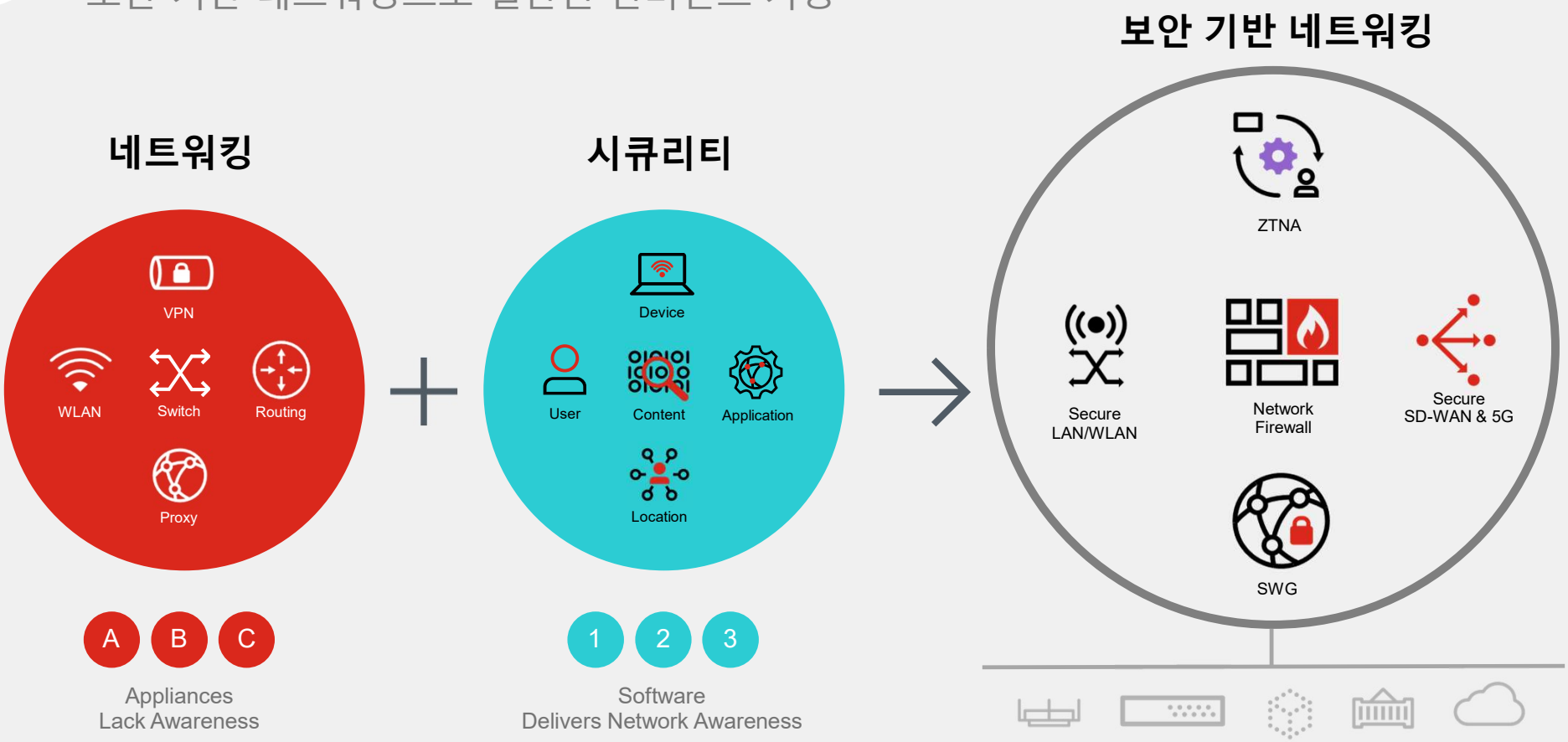
Source: *Gartner "Guide to Cloud Security Concepts"*, Patrick Hevesi, Richard Bartley, Dennis Xu. 21 September, 2021

FORTINET



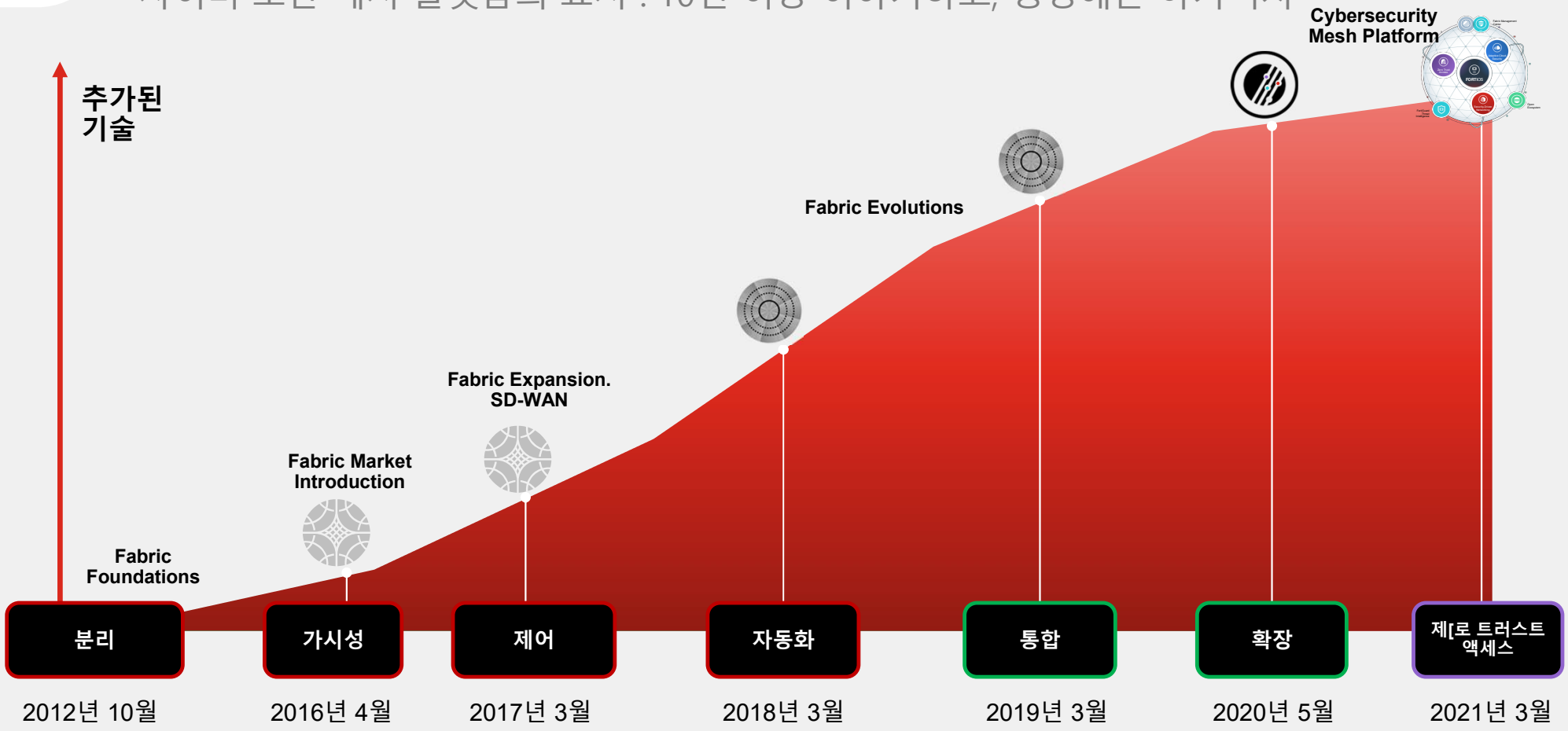
포티넷이 제안하는 컨버전스 접근방식

보안 기반 네트워킹으로 일관된 컨버전스 가능



포티넷 시큐리티 패브릭

사이버 보안 메시 플랫폼의 효시 : 10년 이상 이야기하고, 형성해온 아키텍처



포티넷 솔루션 장점

보안 프로세서

자체 설계 특허
프로세서로 탁월한
차세대방화벽과
SD-WAN 성능과 효율성

FortiOS

포티넷 보안 패브릭의
모든 보안과 네트워킹
요소를 단일 OS에서
구현

보안 패브릭

유기적으로 개발되어
고도로 통합되고
자동화된 사이버보안
플랫폼

에코시스템

300+ 파트너
500+ 통합

FortiGuard Labs: 위협 인텔리전스 및 보안 서비스

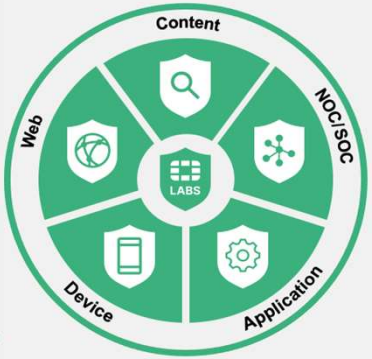
2002년에 설립된 FortiGuard Labs는 포티넷의 엘리트 사이버 보안 위협 인텔리전스 및 연구 조직입니다. 포티넷은 첨단 머신 러닝 및 AI 기술을 개발 및 활용하여 고객에게 시기 적절하고 일관적인 최고의 보호와 실천 가능한 위협 인텔리전스를 제공합니다.

글로벌 리더십 및 협업:

CYBER THREAT ALLIANCE · WORLD ECONOMIC FORUM · INTERPOL · NCI AGENCY

FortiGuard Labs 실시간 위협 정보

FortiGuard AI 기반 보안 서비스



FortiGuard 전문가 서비스

500명+ FortiGuard Labs 글로벌 위협 헌터 및 연구자

600,000시간+ 연간 위협 조사 시간

480개+ TI, 탐지, 적용 및 복구 업데이트 파트너사

포티가드 AI 시큐리티 서비스

- 업계 최고의 보안위협 인텔리전스 및 리서치를 제공하여 포티넷 플랫폼의 보안성을 강화하고 일련의 고급 서비스를 고객에게 전달.
- 31개국에 215명 이상의 연구원 및 분석 전문가 근무
- 200여개의 파트너십 (e.g. Interpol, Certs, etc.)
- 다양한 멀-웨어 및 URL 분석을 수행하고 위협에 대한 모니터링, 분석 및 대응 수행
- Anti-Virus, IPS 엔진 및 시그니처 개발

Global Leadership & Collaboration

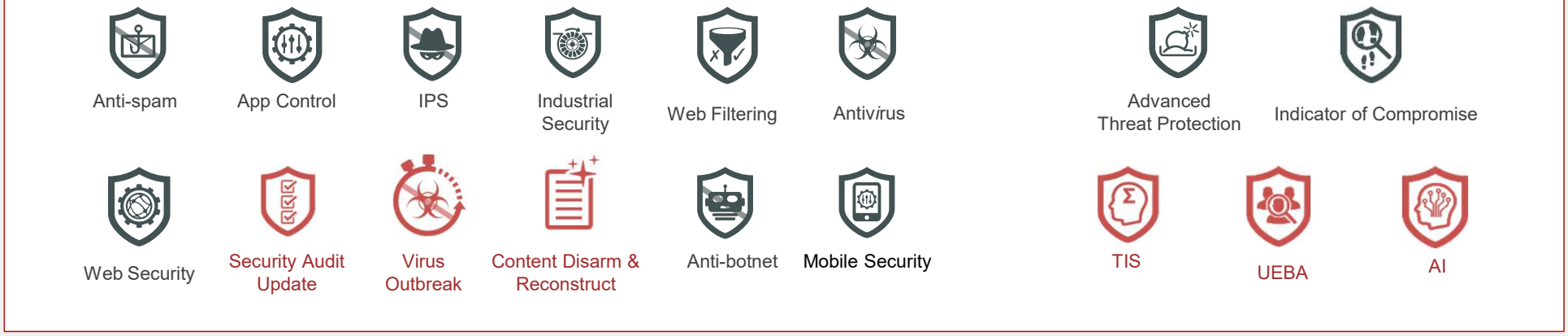
CYBER THREAT ALLIANCE · WORLD ECONOMIC FORUM · INTERPOL · NC AGENCY

Actionable Information and Services

- Incident Response
- Zero Day Research
- Penetration Testing
- Anti-Phishing training
- And More

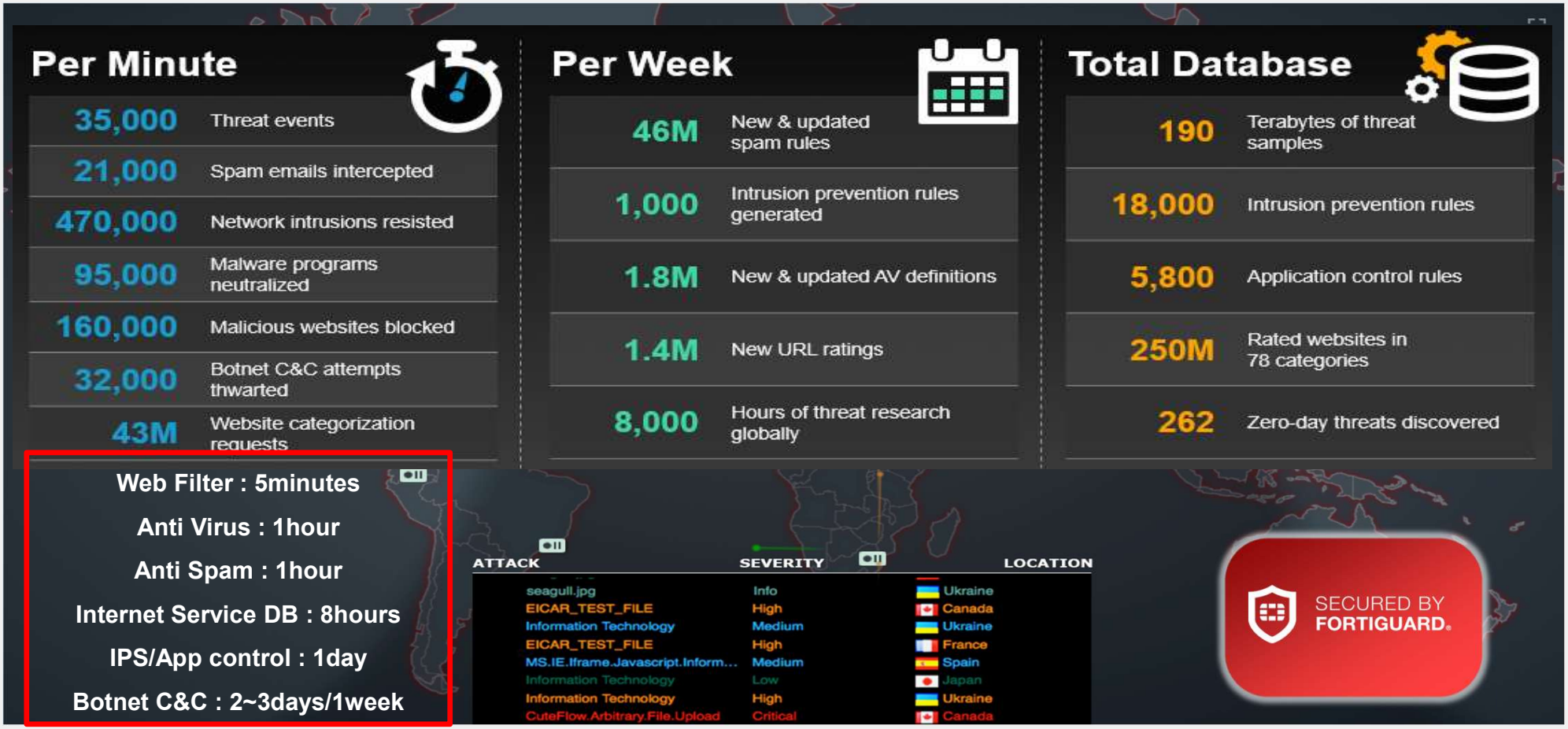
Ai /ML-driven Threat Intelligence

Over 100B global security events analyzed to provide over 1B security updates daily



Protection Services **Detection Services**

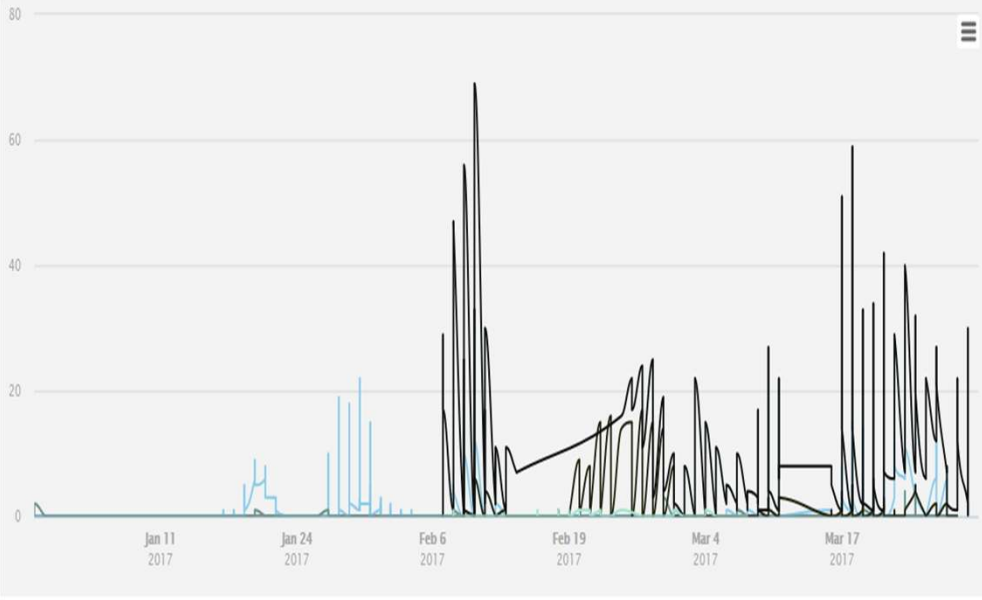
업계 최고 수준 분석 시그니처 업데이트



업계 최고 수준 분석 시그니처 업데이트

- 포티가드-랩은 모든 보안 기술을 자체 개발, 지속적 업데이트
- 독립적이고 실제와 같은 테스팅 환경에서 최상의 보안 효과를 보여줌
- 때문에 사용자 및 단말기들을 보호하는데 최고의 서비스.

THREATS BYPASSING SECURITY PRODUCTS (보안위협 우회 제품들)

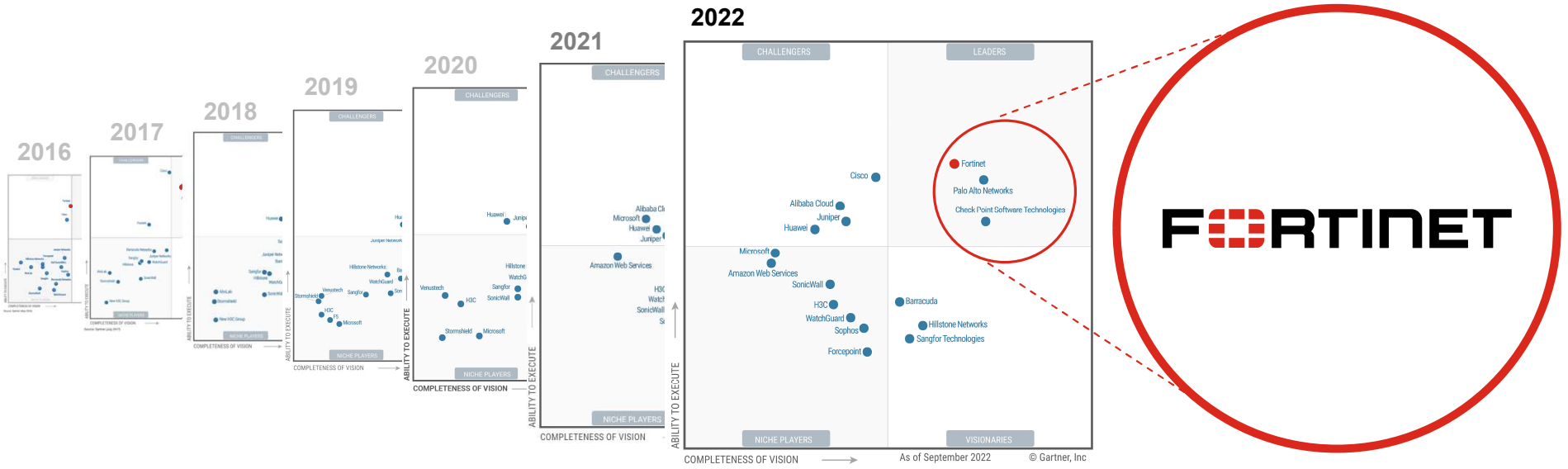


Device	Bypassing
Cisco Meraki NGFW MX64 UTM	1,632
Sophos NGFW Default w/Web Reputation	475
Check Point NGFW 730 UTM	215
Cisco NGIPS Default w/Web Reputation	32
Dell SonicWall NGFW X300 UTM	14
Fortinet NGFW Default w/Web Reputation	0

Source: NSS Labs. Cyber Advanced Warning System.

포티넷 Network Security Leader

네트워크 방화벽, SD-WAN , 유무선 솔루션 등 선두주자로 높은 시장 점유율 확보



7년 연속 네트워크 방화벽의 리더(Leader)로 평가 받는 포티넷의 FortiGate 제품

* 가트너에서 아직 2022년 이후, 2024년까지 Q2까지 가트너 MQ 업데이트 발표 자료 없음

[1] Gartner, Magic Quadrant for Network Firewalls – 2016 – 2022.

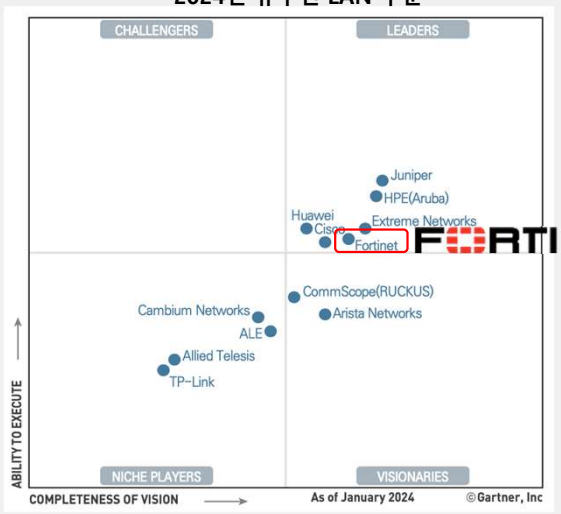
포티넷 Network Security Leader

네트워크 방화벽, SD-WAN , 유무선 솔루션 등 선두주자로 높은 시장 점유율 확보

2024년 네트워크 방화벽 부문

2024년 SD-WAN 부문

2024년 유무선 LAN 부문



과제번호 158 (지정공모형) 과제명 AI·빅데이터 기반 사이버 ...
https://www.kisa.or.kr › jsp › downloadAction.hwp
SOAR* 기술은 기존의 보안 솔루션(SIEM, EDR 등)의 예방·탐지 기능을 포함한 보안 ...
시간은 평균 4.5~15시간이며, 미국 **Fortinet** 제품(자동화)의 경우 20분 소요됨.

○ 정량적 개발목표

	핵심 기술/제품 성능지표	단위	달성목표	국내최고수준	세계 (보유국,
1	AI 기반 이상행위 탐지 정확도	AUC	0.95	-	
2	침해사고 대응 절차 자동화 수행 시간[2]	분	15	-	(미국)
3	보안 위협 대응 시나리오 (플레이북)	개	3,600	-	3 (미국)

세계최고수준 (보유국, 기업/기관명)
0.93[1] (중국/CAS)
20[3] (미국/Fortinet)
3,000[4] (미국/Fortinet)

1) Liu, Fucheng, et al. "Log2vec: A Heterogeneous Graph Embedding Based Approach for Detecting Cyb
Enterprise." Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communication
2) 목표 기술이 침해사고 대응 절차의 자동화 수행 시간을 측정. 보안운영센터(SOC)팀
사고 대응 시간은 평균 4.5~15시간이며, 미국 Fortinet 제품(자동화)의 경우 20분 소요됨.
▪ 침해사고 대응절차 : IOC 식별을 위한 아티팩트 추가 수집, SIEM 이벤트 심사, 장치 격리, 사건 생성 및 분석, IOC 조치, 사고 대응, 요약보고서 작성 등
3) Fortinet, FortiSOAR Empowers Security Operations to Accelerate Incident Response, 2020.
4) Fortinet, FortiSOAR Datasheet, 2020

포티넷 Network Security Leader

네트워크 방화벽, SD-WAN , 유무선 솔루션 등 선두주자로 높은 시장 점유율 확보

엔드포인트 보호

IDC MarketScape Worldwide 현대적 엔터프라이즈용 엔드포인트 보안 공급업체 평가

포티넷이 메이저 플레이어로 선정

Source: IDC, 2024

SIEM

2023년 Gartner Magic Quadrant SIEM 부문

포티넷이 비저너리로 선정

As of April 2021 © Gartner, Inc

SOAR

2023년 GigaOm Radar / Spark Matrix 보안 오케스트레이션, 자동화 및 대응 부문

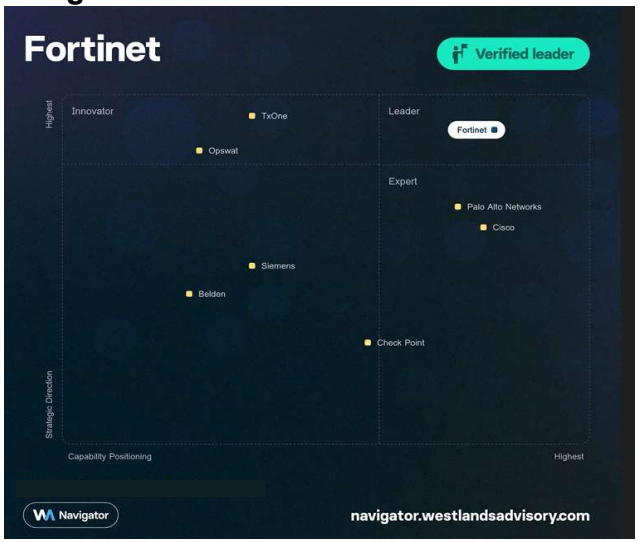
포티넷이 리더로 선정

포티넷 보안 패브릭

포티넷 IT/OT Platforms Leader

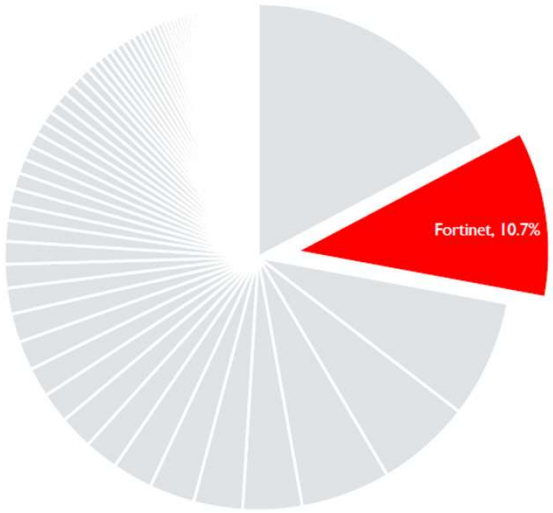
IT/OT 보안 플랫폼 내비게이터 2023의 유일한 리더로 시장 점유율 확보

IT/OT Network Protection Platforms Navigator 2023



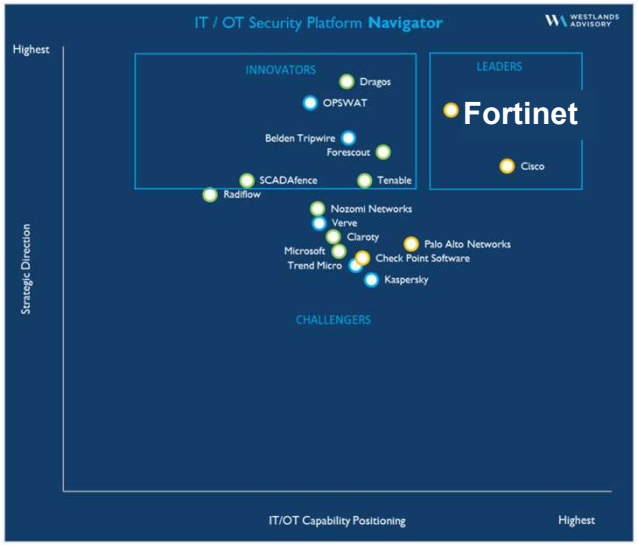
WESTLANDS ADVISORY

Market Share Profile
IT/OT Convergence TAM, 2022



WESTLANDS ADVISORY

IT/OT Security Platform Navigator 2022



Primarily NGFW & Zero Trust
Mixed Capabilities
Primarily Vulnerability Management & Threat Detection

WESTLANDS ADVISORY

인정받은 업계 인지도

	FORTINET	cisco	paloalto NETWORKS	JUNIPER NETWORKS	Symantec	Check Point SOFTWARE TECHNOLOGIES LTD.
Gartner Magic Quadrant	12*	7	3	4	3	2
NSS LABS RECOMMENDED	9	4	5	1	0	2

* https://docs.google.com/viewer?url=https%3A%2F%2Fwww.fortinet.com%2Fcontent%2Fdam%2Ffortinet%2Fassets%2Fbrochures%2Fbrochure-analyst-recognition.pdf

인정받은 업계 인지도

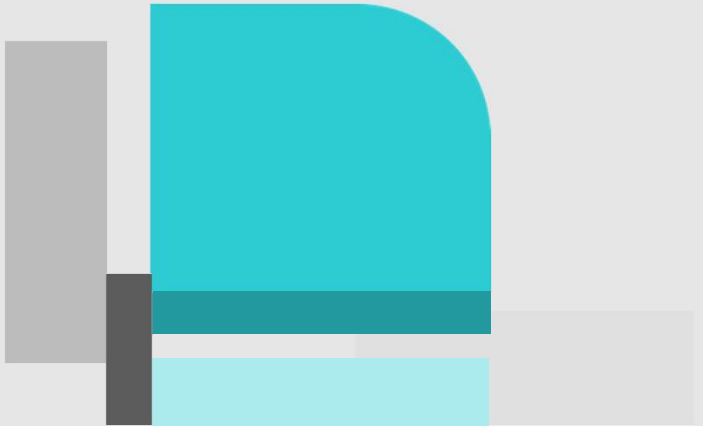
33개

엔터프라이즈 애널리스트 보고서로 포티넷 네트워킹 및 보안 역량 검증

포티넷은 수십 개의 애널리스트 보고서에서 선두를 지키며 가장 많은 검증을 받은 세계적인 엔터프라이즈 사이버 보안 기업 중 하나로, 이들 보고서에는 포티넷 보안 패브릭의 광범위한 적용 범위가 잘 나타나 있습니다.

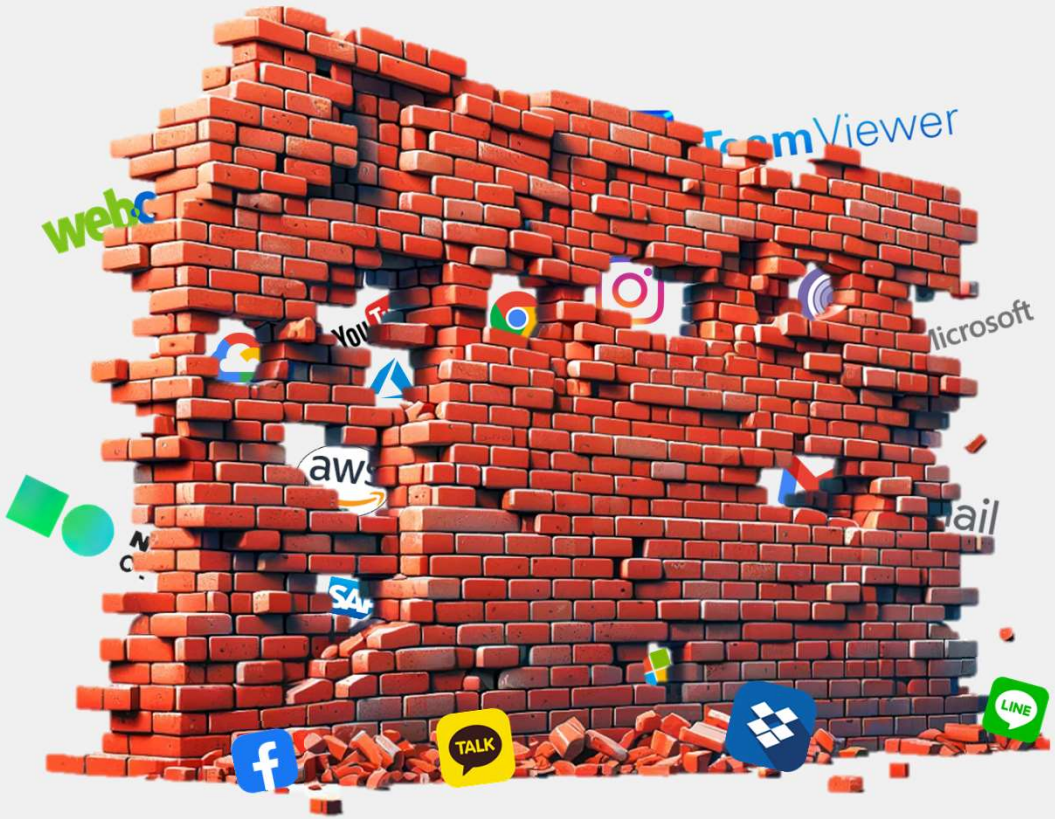
- 네트워크 보안 및 액세스 제어
- 유무선 액세스
- ID 및 액세스 관리
- 이메일 및 애플리케이션 보안
- 하이브리드 클라우드 보안
- 엔드포인트 보안
- 조기 및 지능적 탐지
- 중앙 분석 및 대응 워크플로

포티넷 차세대 방화벽



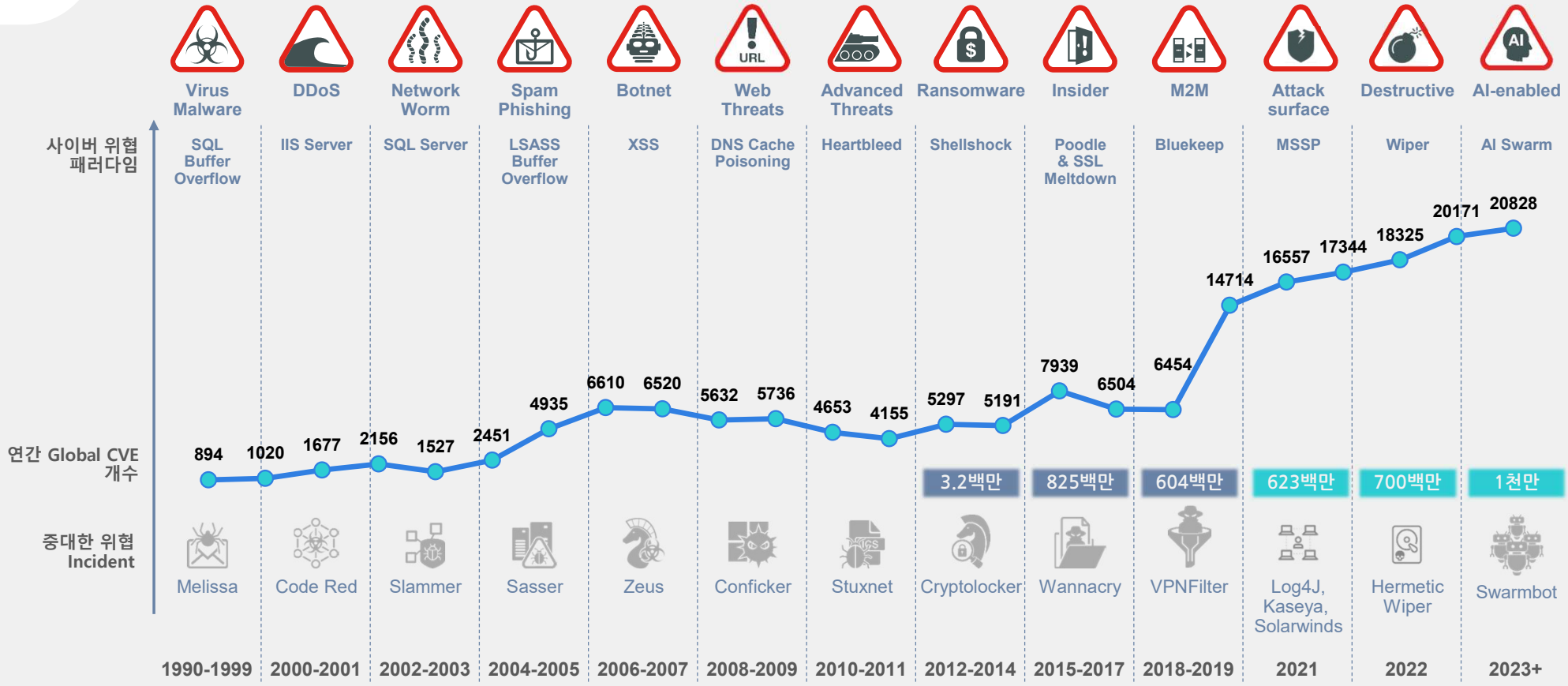
DX로 심화되는 기존 방화벽의 한계

차세대 방화벽(NGFW)를 사용해야 하는 이유



- **Application 진화**
  - 특정 IP와 port에 고정되지 않는 진화된 Application 다수 등장
  - IP와 port 기반으로 설정하는 기존 방화벽은 Application에 대한 통제 불가
- **보안 기능 부족**
  - 진화하는 APT 공격 및 Zero-day 취약점에 대한 방어 대응 필요
  - 기존 방화벽은 IPS와 Anti-Virus 기능을 제공하지 않아 별도 장비가 따로 필요하며, 그로인한 운영 복잡성 증가
- **트래픽 가시성**
  - SSL을 이용한 암호화된 트래픽에 대한 가시성 확보 불가
  - 어플리케이션 레벨의 실시간 트래픽 정보와 실시간 위협정보 제공 불가

보안 위협에 AI를 이용하기 시작

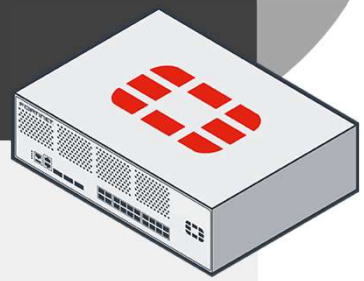


2023년 데이터 유출의 평균 비용이 사상 최고치인 445만 달러에 달했습니다.[1]

[1] Ponemon Institute, Cost of a Data Breach Report, 2023

FortiGate NGFW

- ✓ **Fortinet 전용 ASIC 하드웨어** 칩과 멀티 CPU 최적화 방화벽으로 **Latency를 최소화**(2~4μs)
- ✓ 시장이 평가한, 업계 **최고수준의 보안 및 네트워킹의 융합을 구현**한 제품
- ✓ 전통적인 방화벽의 기능에 더해 최소 **10가지 이상의 고급 위협 방지기능**을 탑재
- ✓ **한 제품으로 다중 Use-Cases를 지원하는 차세대방화벽**



타의 추종을 불허하는 성능 및 보안

업계 평균을 상회하는 포티넷의 최신 ASIC 기술

Content Processor 10

컨텐츠 검사 및 암/복호화 H/W 처리속도 가속

Network Processor 7

네트워크 트래픽 처리 및 라우팅 가속화, 레이턴시 최소화

Security Processor 5

네트워크 및 콘텐츠 처리를 통합하여 비용 효율적 고성능 제공

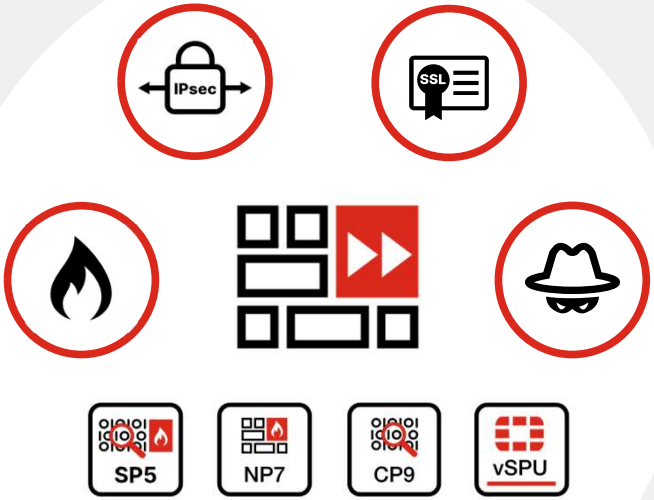
SPU는 많은 이점을 제공

Better Performance in a Key RFP Item!	Better Visibility for DIA!	Lower OpEx and Hit ESG Goals!	Let IT Bring Value to the Business!
			
Up to **9X** Threat Protection	Up to **10X** SSL / TLS	Energy Consumption Reduced **60%**	**40%** Reduction in TCO

ASIC 가치에 대한 이해

Deliver user experience
in **consumer devices**

Mobile ASICs

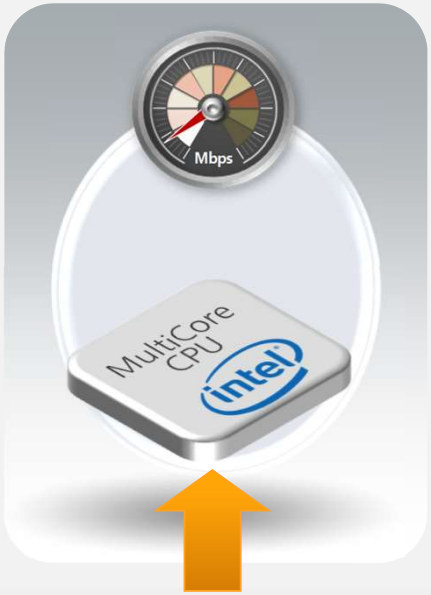


Deliver user experience
in **edge devices**

Networking & Content ASICs

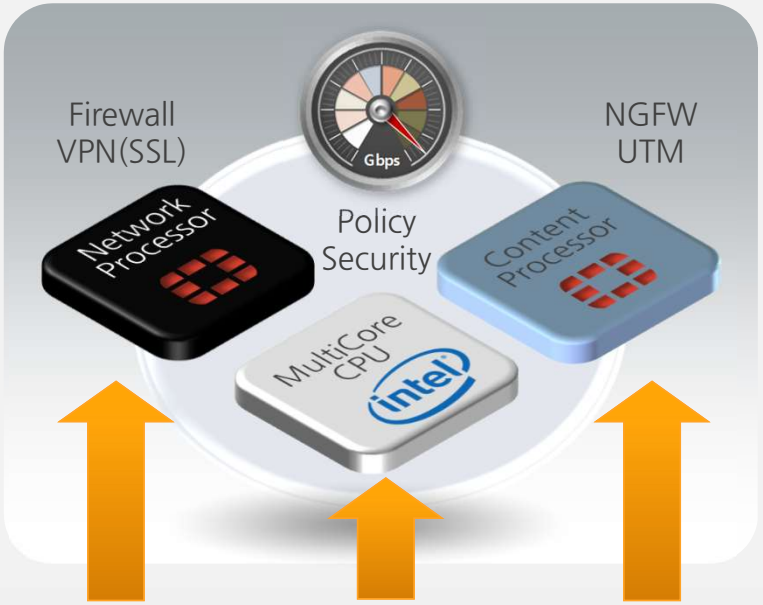
전용 ASIC 기반의 고성능/저지연 방화벽

국산 등 경쟁사 방화벽
아키텍처 멀티 CPU 최적화



CPU
방화벽 정책, 콘텐츠 검사, 암복호화 및 패킷 처리

포티넷 방화벽 아키텍처
전용 ASIC 하드웨어 칩과 멀티 CPU 최적화
방화벽 Latency 최소화 (2~3㎲)



Network Processor
방화벽 정책과 VPN 트래픽의 H/W 가속

CPU
방화벽 정책 처리

Content Processor
콘텐츠 검사 및 암복호화 H/W 가속

Fortinet Parallel Path Processing

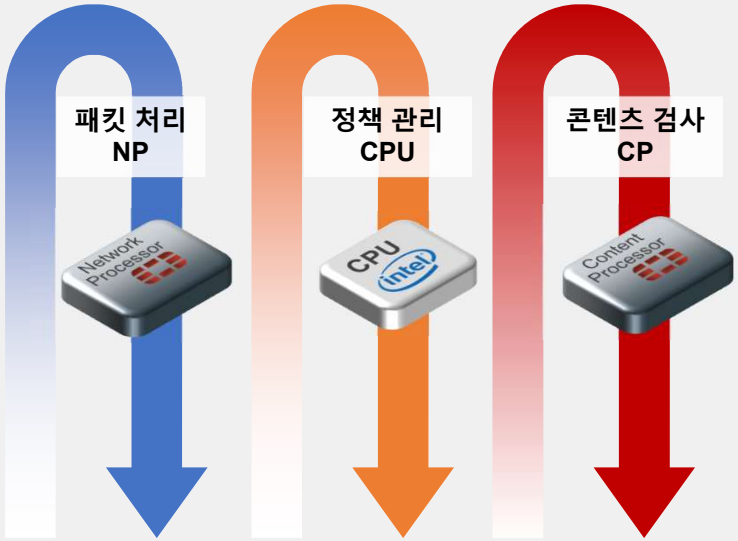
- 성능 개선
- 지연 감소
- 공간 절약
- 적은 전력

성능 저하 최소화 구조

타사 CPU only vs. 포티넷 ASIC 기반

CPU Only

Fortinet PPP (Parallel Path Processing)



- 성능 개선
- 지연 감소
- 공간 절약
- 적은 전력

전용 ASIC 기반의 고성능/저지연 방화벽

타사 CPU only vs. 포티넷 ASIC 기반

CPU 및 직렬 처리 기반

방화벽 → 6 Gbps

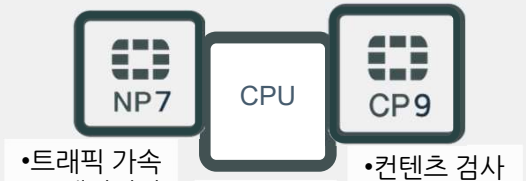
VPN → 2 Gbps

IPS → 3.5 Gbps

Intel E5 2640v2 기반
(8 코어 2GHz)

VS.

Fortinet SPU 기반 병렬 경로 처리



방화벽 → **40** Gbps

IPSec VPN → **25** Gbps

SSL VPN → **28** Gbps

IPS → **20** Gbps

6 ~ 12배 성능

Fortinet SoC
(System-on-a-Chip)

기본형 폼팩터로 최적화됨

5배 Gbps

8/11배 IPSec/SSL VPN

5배 IPS 성능

5배 동시 세션

3배 전원 효율성

성능 개선

지연 감소

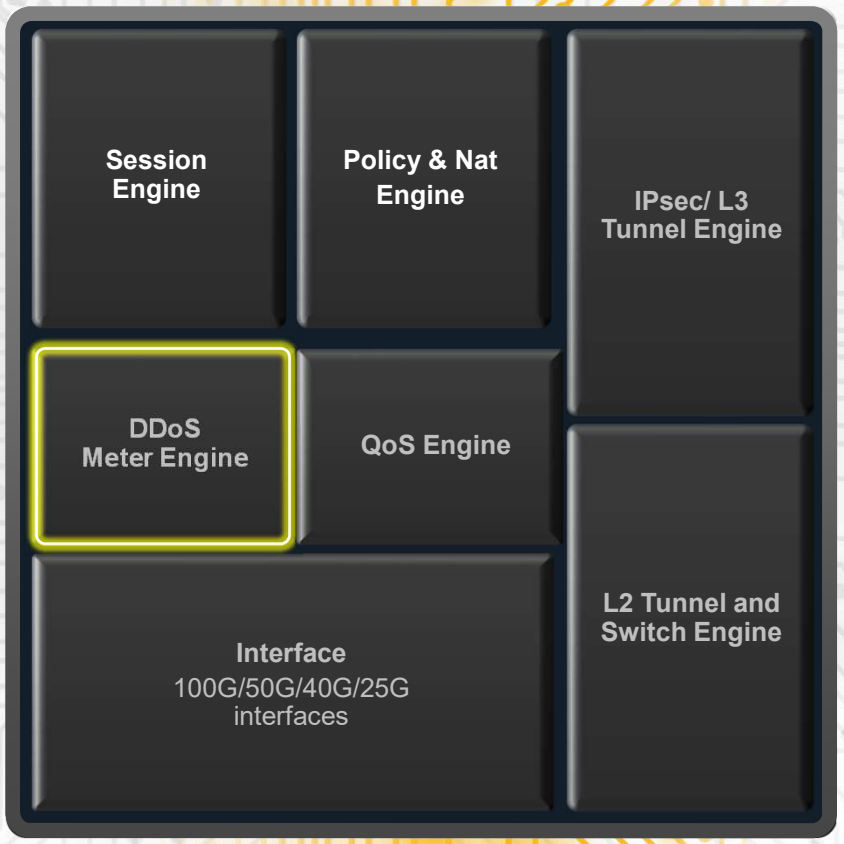
공간 절약

적은 전력

NP : DDoS 공격방어

Zero CPU
DDoS Protection

CPU 부하 없는
DDoS 공격으로 부터의
시스템 보호

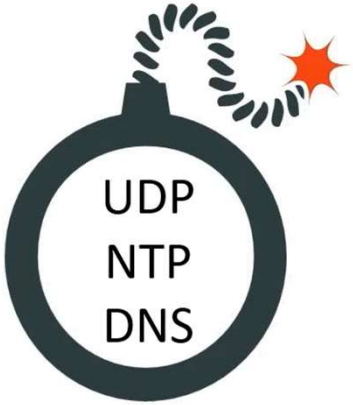


© Fortinet Inc. All Rights Reserved.

NP : DDoS 공격 방어

가장 큰 DDoS 공격
1.3 TBPS

가장 많은 유형의
공격 형태



연간 기업의
손해 비용

© Fortinet Inc. All Rights Reserved.

FortiGate NGFW Appliance

다양한 규모의 고객 환경을 보호하기 위한 업계에서 가장 광범위한 NGFW 포트폴리오

Branch
(40-90 Series)

POE
SSD
DSL
LTE
WI-FI
Bypass

OT Deployments

Bypass
Rugged

FG-40F Series
0.6 Gbps
Threat Protection

FG-60F Series
0.7 Gbps
Threat Protection

FG-80F Series
0.9 Gbps
Threat Protection

FG-90G Series
2.2 Gbps
Threat Protection

Campus
(100-900 Series)

FG-100F Series
1.0 Gbps
Threat Protection

FG-200F Series
2 Gbps
Threat Protection

FG-400F/ FG-600F Series
9-10.5 Gbps
Threat Protection

FG-900G Series
20 Gbps
Threat Protection

Data Center
(1000-4000 Series)

Large Data Center
(6000-7000 Series)

FG-1000F Series
13 Gbps
Threat Protection

FG-1800F Series
15 Gbps
Threat Protection

FG-2600F Series
15 Gbps
Threat Protection

FG-3200F Series
45 Gbps
Threat Protection

FG-3500F Series
63 Gbps
Threat Protection

FG-3700F Series
75 Gbps
Threat Protection

FG-4000F Series
45 – 70 Gbps
Threat Protection

FG-6300F Series
60 Gbps
Threat Protection

FG-6500F Series
100 Gbps
Threat Protection

FG-7000F Series
50 - 520 Gbps
Threat Protection

다양한 규모의 고객환경을 고려한 광범위한 제품 라인업

SD-WAN과의 통합 | 고 성능 SSL inspection | 업계 평균의 4배 이상 위협 보호

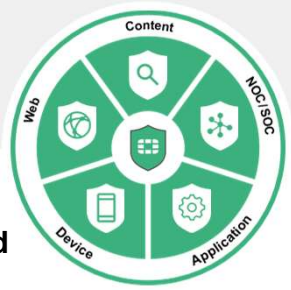
Enterprise 고객환경을 위한 고사양 제품 라인업

ZTNA 통합 | VXLAN 배포 | <2 us Ultra-low latency | 400GE Built-in Ports

SP5 **네트워크 및 보안 융합 가속화**

CP9 NP7 **FortiASIC을 통해 최대 88%의 전력 소모율 감소**

FortiGaurd AI-powered Security



FortiGuard

Content Security

AV | IL MPS | DLP

Web Security

DNS | URL | BOT

Device Security

IPS | OT | IoT

NOC/SOC

IoC | SEC RATING

Application Security

IL CASB | APP CTRL

FortiGate Bundles

Advanced Threat Protection

Network & File Security
IPS
Anti-Malware
Application Control

Unified Threat Protection

Web/DNS Security
Web Filtering
IP & Botnet C&C
DNS Security

NEW Enterprise Protection

SaaS & Data Security
DLP
Inline CASB
IOT Security
Security Rating

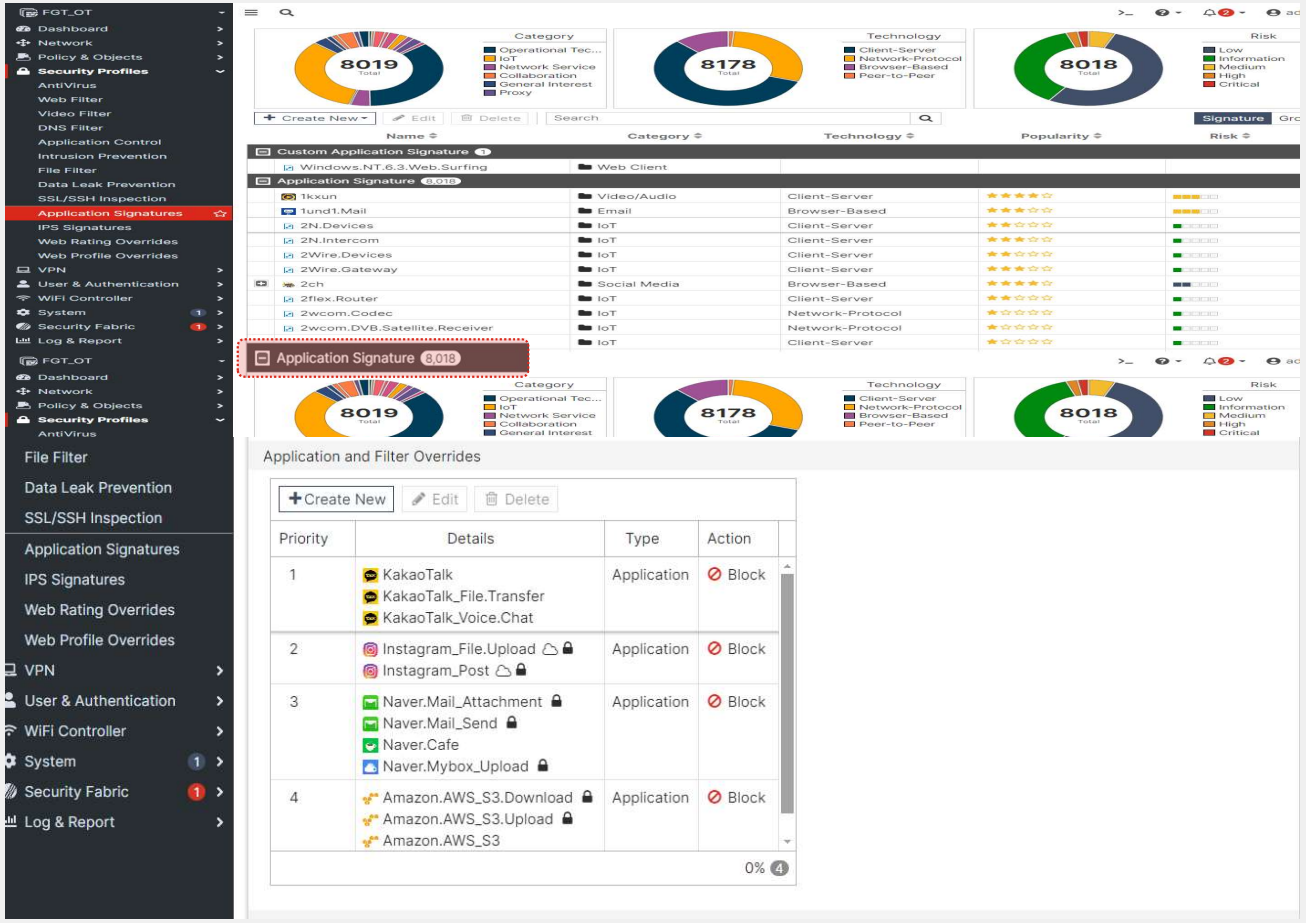
Zero-Day Prevention
AI-based Inline Malware Prevention
Plus: FortiConverter

FortiCare Premium

Application control

- **상용 소프트웨어의 고도화**
  - 수많은 Application이 다양한 니즈에 의해 개발되고 만들어지며, 클라우드를 사용하는 App 등, **특정 IP와 port에 고정되지 않은 서비스가 꾸준히 증가**하고 있음.
  - 이에 따라 전통적인 방화벽은 더 이상 Application을 통제 할 수 없음
  - 내부 사용자/디바이스가 사용하지만, 보안 담당자가 모르는 Application은 보안에 가장 큰 위협 요소가 됨

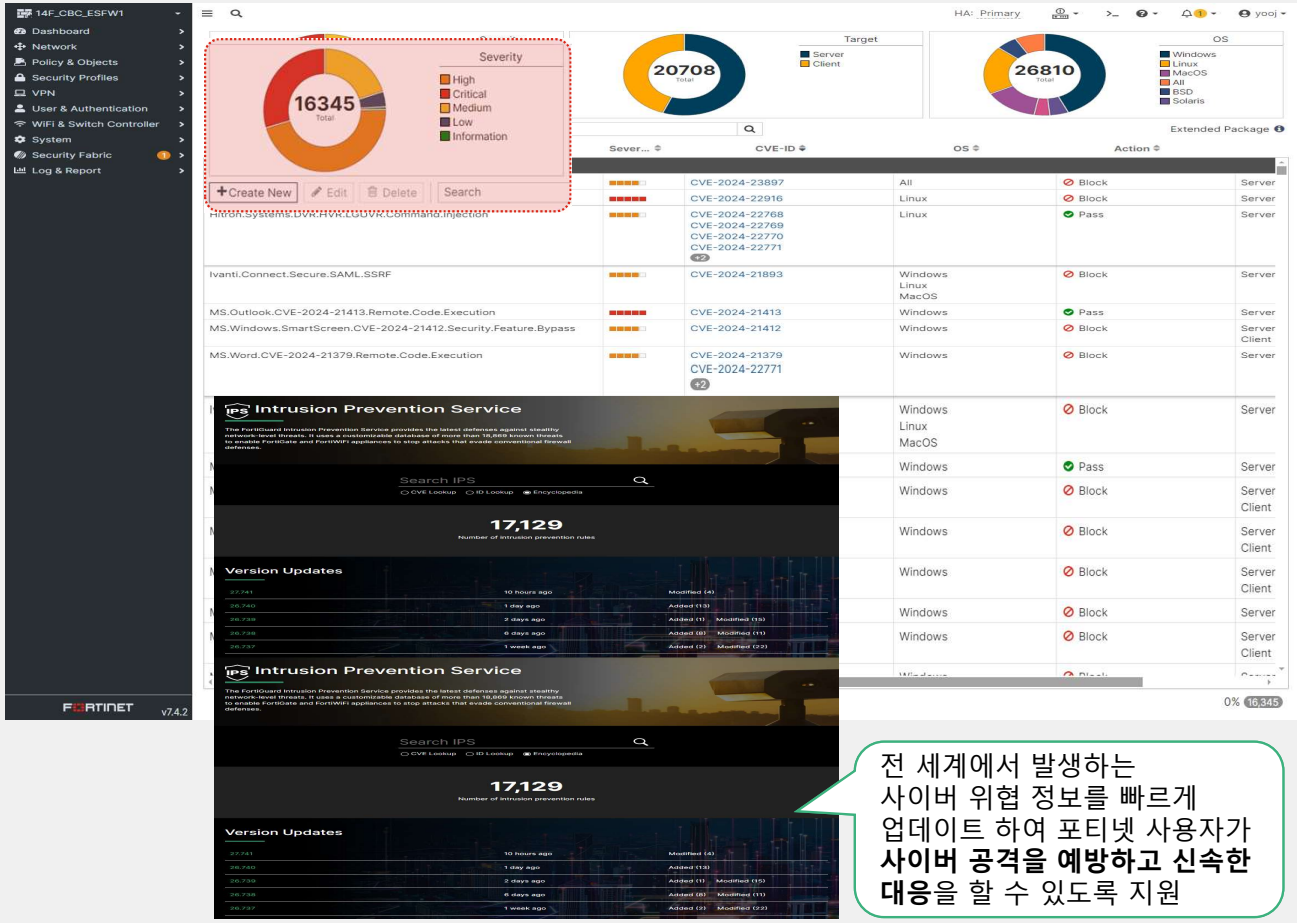
- **FortiGate App Control**
  - **8,000여개 이상의 App control 패턴** 제공
  - 통신 패턴 분석을 통해 고객사만의 커스텀 Application 시그니처 생성 가능



Intrusion Prevention(IPS)

- **증가하는 공격 시도와 다양화되는 패턴**
  - 사이버 위협은 갈수록 복잡해지고 집요해지고 있으며, 그 예로 **연간 CVE 취약점 발견 개수는 급격한 상승 곡선**을 그리고 있음
  - 다양한 시도로 비즈니스의 연속성을 해치려 하고 있으나 고급 IPS 장비를 별도로 구축하는 것은 비용 효율적이지 못하고, 많은 네트워크 문제를 야기시킴.

- **FortiGate IPS Engine**
  - 보안 컨텐츠 검사에 특화된 ASIC(CP)칩셋을 사용하여 **대량 패턴매칭을 위한 고속처리 지원**
  - **17,000여개 이상의 IPS 탐지 시그니처** 제공
  - 통신 패턴 분석을 통해 고객사만의 커스텀 Application 시그니처 생성 가능

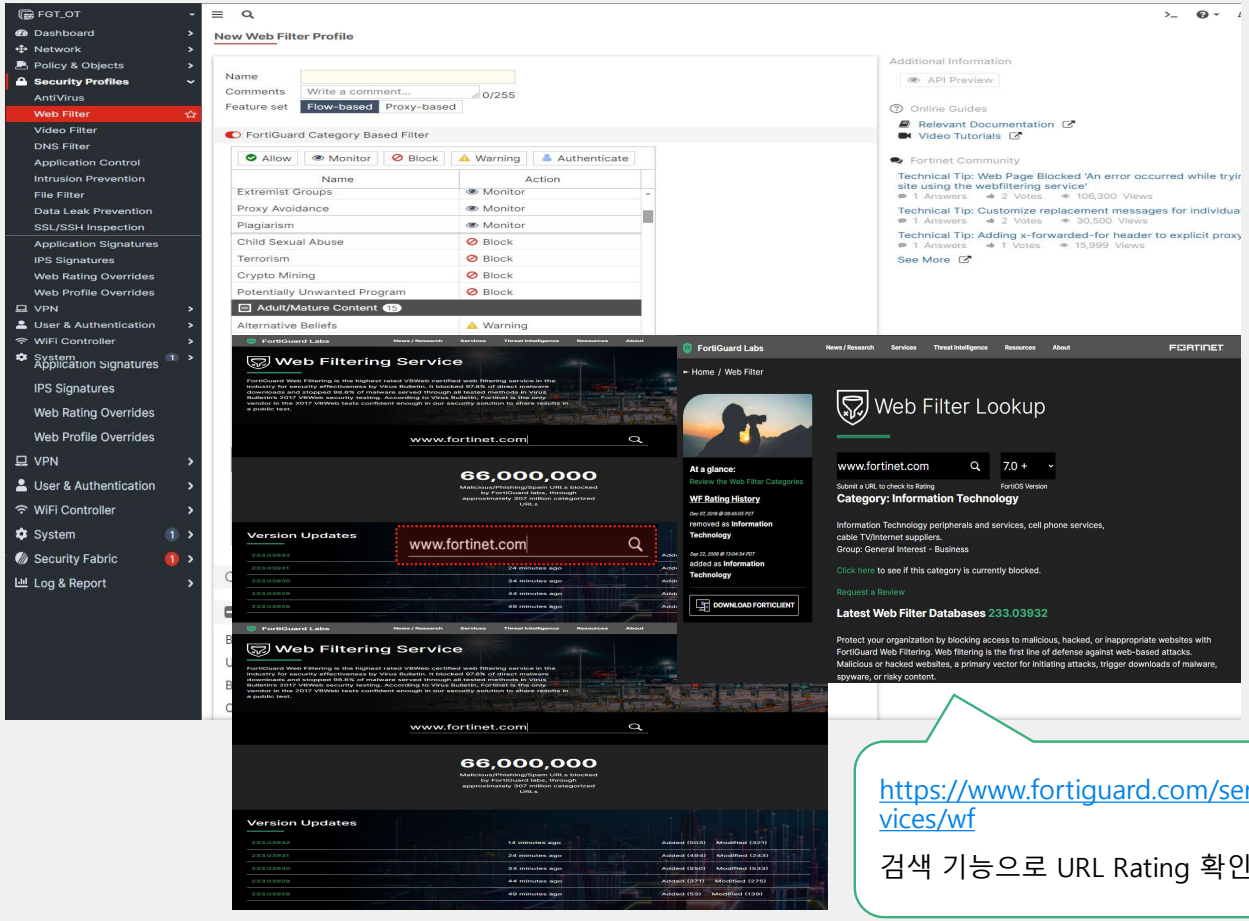


전 세계에서 발생하는 사이버 위협 정보를 빠르게 업데이트 하여 포티넷 사용자가 **사이버 공격을 예방하고 신속한 대응**을 할 수 있도록 지원

Web Filter

- **전통적인 웹 기반 공격으로부터의 보호**
  - 악성 코드를 다운로드 받는 C&C, Botnet Site, 클릭을 유도하여 스크립트를 실행시키는 피싱 사이트, 스파이웨어/백도어를 호스팅하는 웹사이트와 같은 위험한 웹 사이트 등
  - 이러한 웹사이트는 IP를 수시로 변경하여 추적이 어렵고, 전통적인 방화벽으로는 이를 통제할 수 없음.

- **FortiGate Web Filter**
  - 전 세계에서 신규로 발생하는 URL에 대한 빠른 업데이트 지원(5분 간격으로 Update)
  - **약 3억 개의 URL Database 보유**
  - 6,600만개의 악성/피싱/스팸 URL 차단 지원

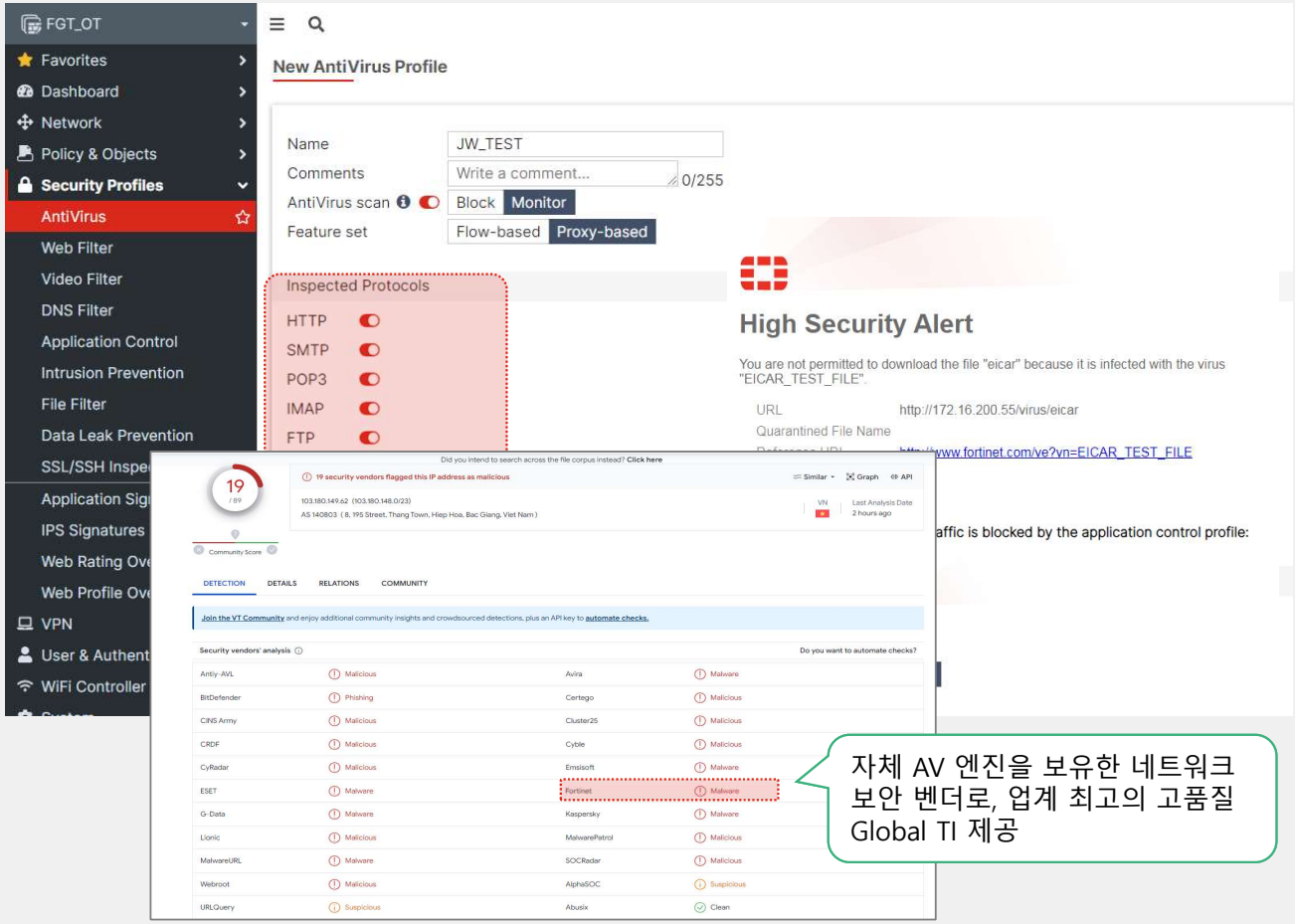


https://www.fortiguard.com/services/wf

검색 기능으로 URL Rating 확인

Anti-Virus

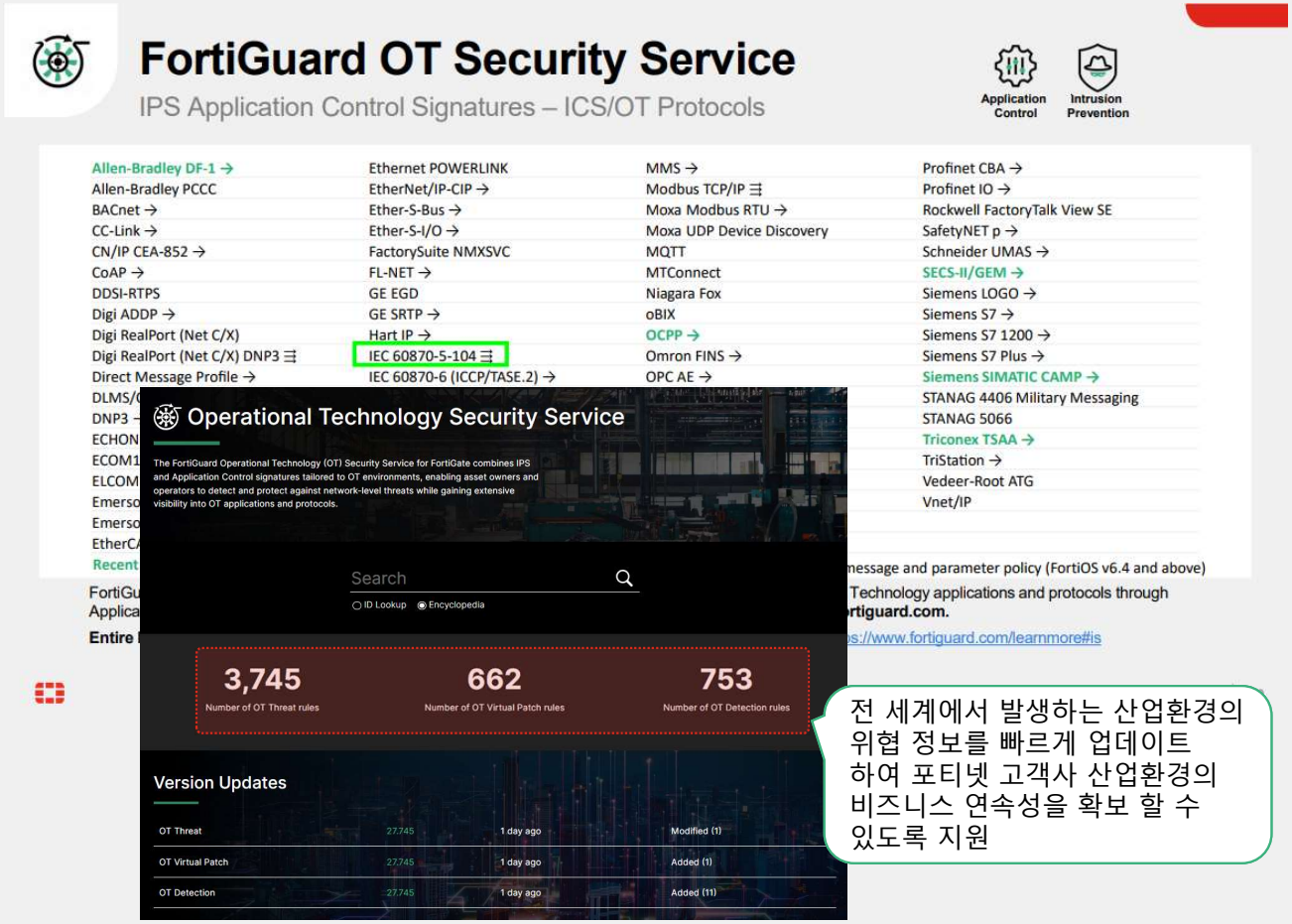
- **FortiGate Anti-Virus Profile**
  - 포티넷은 세계 TOP10 자체 AV 엔진을 보유한 유일한 네트워크 보안 벤더이며, 국제 공인 Virus 평가기관에서 검증됨.
  - Anti-Virus 엔진과 Anti-Virus 시그니처를 모두 자체 개발하며, 업계 최고 수준의 Update 주기(1시간)를 지원
  - FortiGuard에서 제공하는 Anti-virus서비스는 기존의 서명 기반 탐지 방법보다 진화한 **CPRL(콘텐츠 패턴 인식 언어)**을 사용
  - 포티넷에서 특허 받은 CPRL의 장점은 특정 코드 문자열 일치에만 국한되지 않기 때문에 높은 Proactive 탐지율을 지원



OT Security Service

- **폐쇄 환경에서 4차 산업혁명으로 인한 DX**
  - 가용성을 중시하여 폐쇄적으로 운영되던 다양한 산업/사회 인프라망이, 다양한 니즈에 의해 인터넷에 연결되고 있음
  - 30~40년간 조금씩 진보되어 온 IT 보안체계 (OS 핫픽스, 보안 패치, 보안 장비)에 대해 **갑작스럽게 많은 부분을 적용하기 힘든** 환경
  - 전통적인 방화벽으론 산업용 제어 시스템의 산업 통신 프로토콜과 제조사 독점 프로토콜을 확인 할 수 없어 **외부 위협에 그대로 노출**됨

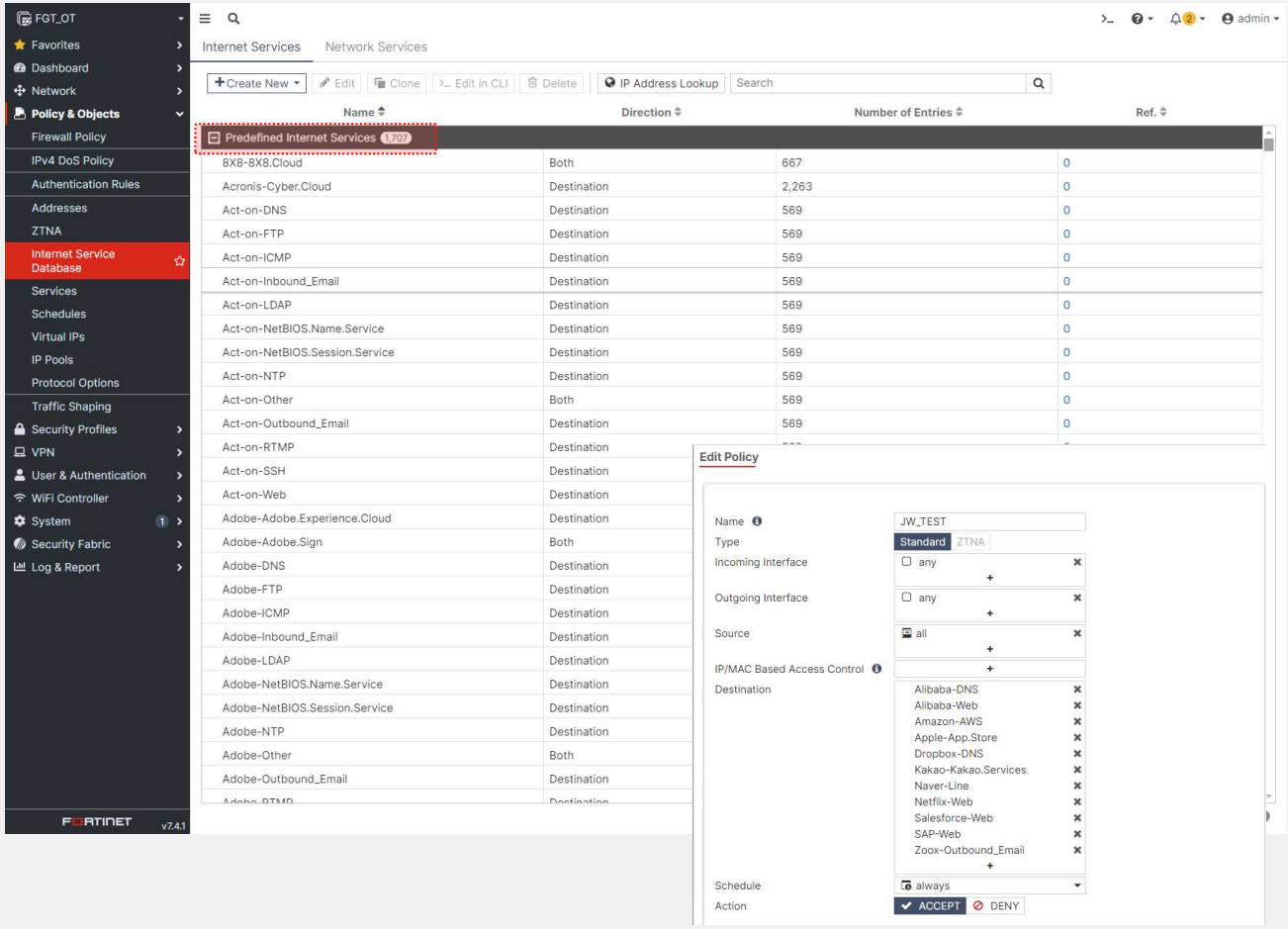
- **FortiGate OT Security Service**
  - **약 3천개의 Protocol Decoder(App.Cont) 지원**
  - **약 600개의 Virtual Patch(OT.IPS) 패턴 지원**
  - 내부 자산을 시각화 하는 Asset Identity Center



전 세계에서 발생하는 산업환경의 위협 정보를 빠르게 업데이트 하여 포티넷 고객사 산업환경의 비즈니스 연속성을 확보 할 수 있도록 지원

Internet Service Database

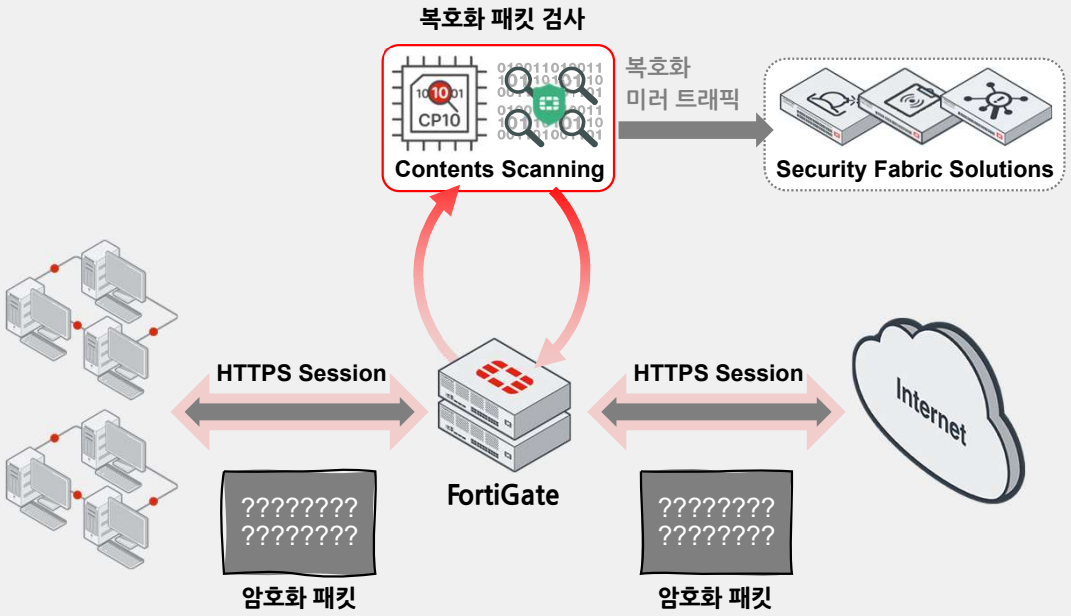
- **FortiGate Internet Service Database**
  - 잘 알려진 인터넷 서비스는 불특정 다수에 대해 높은 수준의 서비스를 제공해야 하기 때문에, 웹 서비스의 IP/Port를 많이 사용함.
  - FortiGate에서는 이러한 수만 여개의 IP/port 정보를 자체 DB로 제공하여, **편리하게 해당 서비스명을 방화벽 객체로 사용**할 수 있음
  - **Geo-based 옵션 :** 사용하는 국가별로 Internet Service DB를 분리하여 설정 및 사용하는 기능 제공
  - **별도의 라이선스 없이 사용 가능**



FortiGate - SSL Full Inspection

- **정보보안을 위한 암호화, 위협도 암호화**
  - 구글의 웹사이트 중 95%가 HTTPS를 사용하며, 보안 위협 중 85%의 위협이 암호화 되어있음*
  - 암호화가 데이터 보호에 기여할 수 있지만, 동시에 사이버 위협을 숨기는 수단으로도 사용될 수 있으며, 전통적인 방화벽으로는 성능의 한계로 온전히 대처할 수 없음

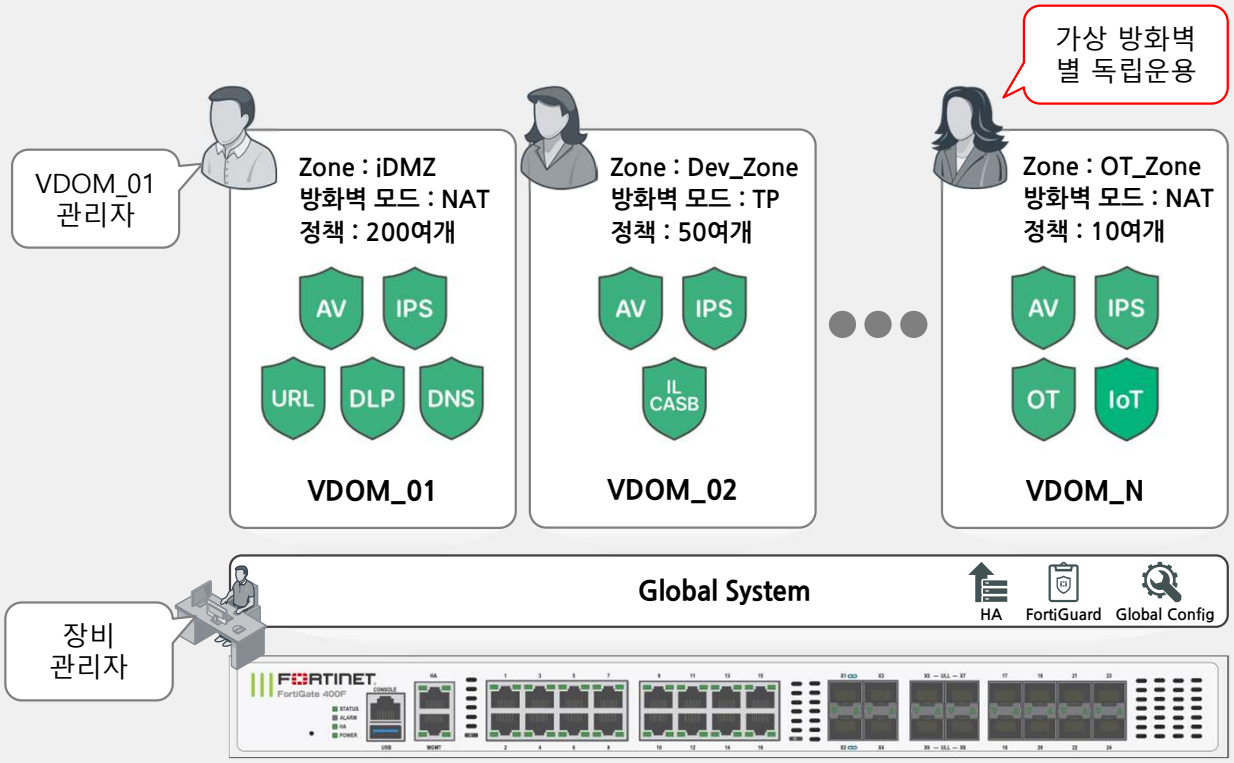
- **FortiGate SSL Full Inspection**
  - 자체 ASIC(CP)을 통한 SSL Full Inspection 기능을 제공하여, 암호화된 통신을 고속으로 복호화 하고, 차세대 방화벽의 보안기능 활용
  - 다른 보안 시스템에 복호화 트래픽을 전송하여 HTTPS를 처리하지 못하는 장비의 활용성 증가



※ 출처 : https://serpwatch.io/blog/ssl-stats/#stat19

FortiGate - 자체 가상화(VDOM)

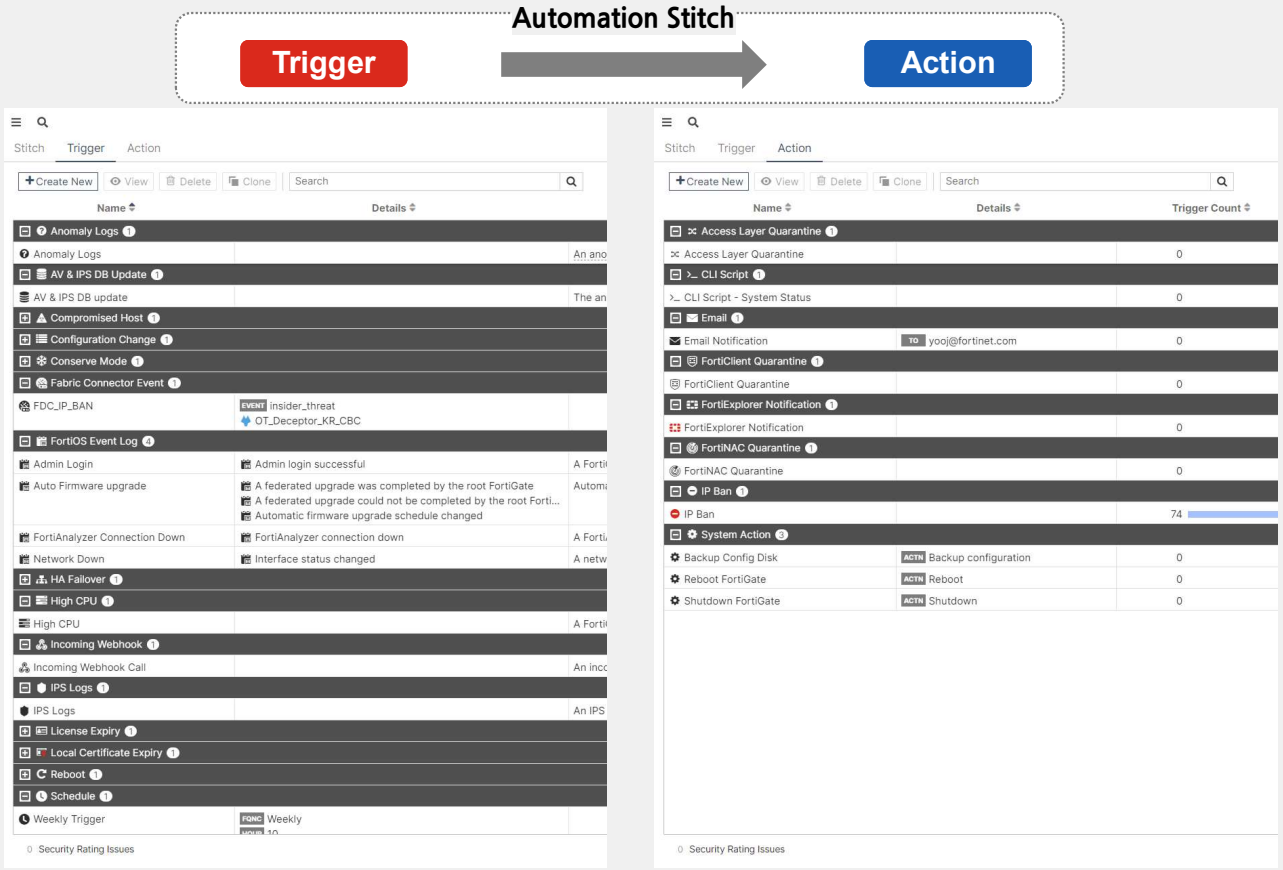
- **FortiGate VDOM 기능**
  - 1대의 물리적 방화벽을 **논리적으로 여러 대로 나누어 방화벽 기능과 정책이 독립적으로 동작하도록 설정**하는 기능
  - 가상 방화벽별로 NAT/TP(L3/L2) Mode 및 주요 보안기능 On/Off
  - 가상 방화벽 별 별도 관리자 지정 기능
  - 가상 방화벽 별 특정 권한 부여 계정 제공
  - 가상 방화벽 별 별도 Logging 기능
  - 물리적 공간의 한계와 전력 효율 감소 효과
  - 네트워크 망 분리를 많이 해야 하는 상황(e.g OT ISFW)에서 비용 절감을 위해서도 활용
  - **별도 라이선스 없이 10개까지 사용가능**(최대 250개)



FortiGate - Automation Stitch

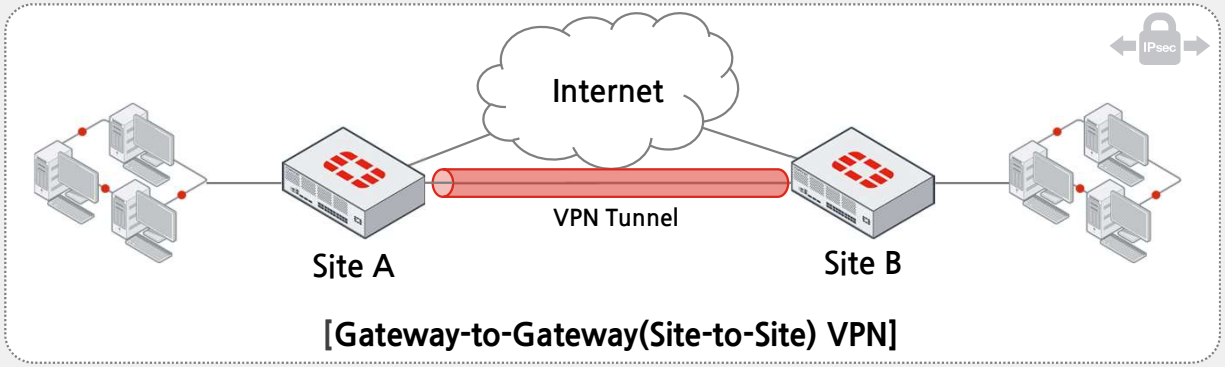
- **FortiGate 운영 자동화 지원 기능**
  - 1개의 이벤트 트리거와 1개 이상의 액션을 묶어서 사용
  - 이벤트 트리거 발생시 자동으로 사전 정의한 액션을 수행하여 편리하고 자동화된 운영 지원
  - **별도 라이선스 없이 사용 가능**

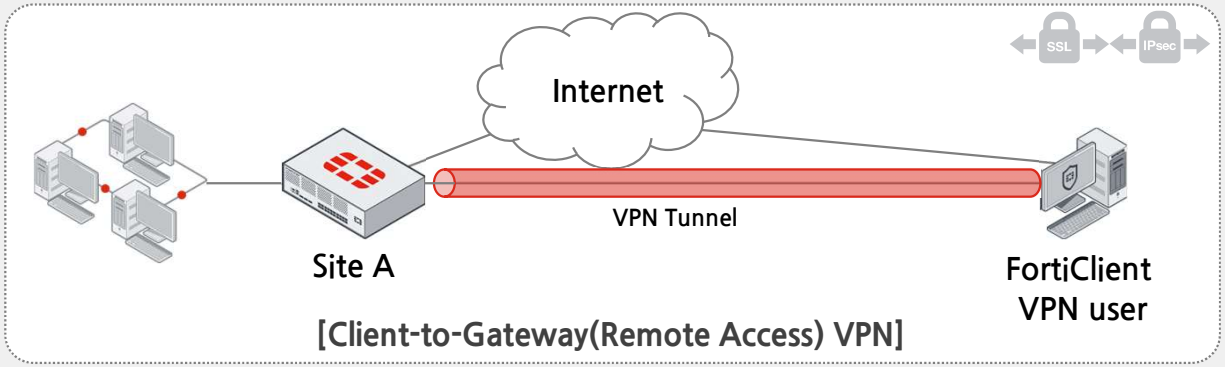
- **사용 예시**
  - FortiGate에서 특정 이벤트 로그 발생시 관리자에게 Email / SMS 발송
  - FortiGate CLI 설정을 Trigger 또는 스케줄에 따라 수행
  - 연동된 제품으로 특정 이벤트가 수신되면, 해당 호스트를 일정시간동안 Quarantine
  - 클라우드 API 또는 Webhook 수행



FortiGate - VPN Gateway

- **Fortinet VPN 기술**
  - FortiOS의 IPsec 및 SSL VPN은 인증된 사용자를 식별하고 리소스에 대한 액세스 제어
  - VPN은 내부 사용자 데이터베이스 또는 외부 LDAP, RADIUS, TACACS+, PKI, Windows AD 서버와 연동하여 사용자 인증 제공
  - 사용자를 위한 FortiClient VPN 프로그램 제공
  - **SSL VPN을 포함하여, 별도 라이선스 없이 사용 가능**



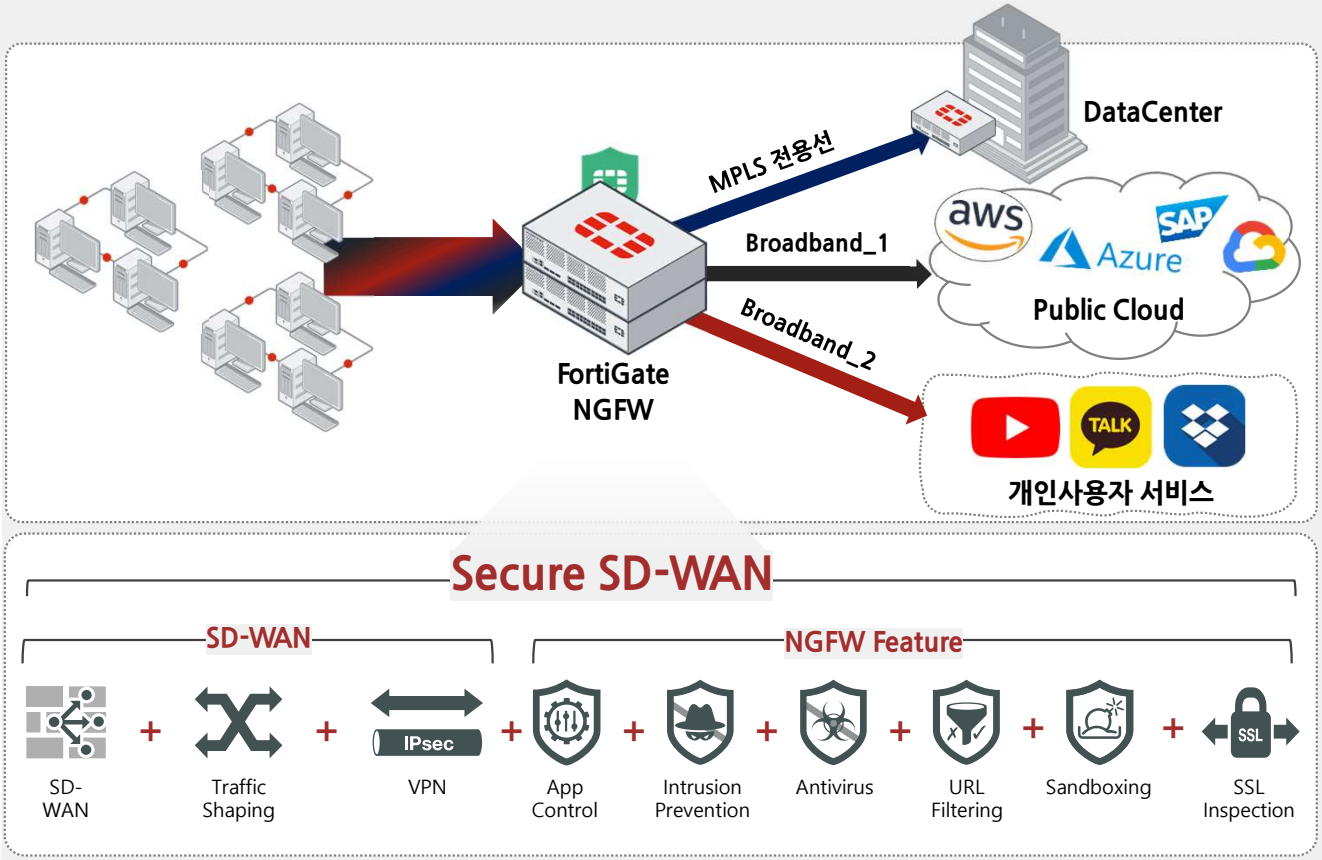


※ 자세한 내용은 FortiGate VPN 소개자료를 추가로 참조하세요

FortiGate - Secure SD-WAN

- **업무의 연속성 강화로 고객 만족도 향상**
  - 전용선, 인터넷 등 회선에 대한 품질 모니터링을 통해 최적의 경로 선택 및 회선 사용 최적화
  - 주요 어플리케이션 별 우선 순위를 부여하여 사용자 만족도 향상
  - 각 Branch별 상태 모니터링 및 통합관리
  - 멀티 클라우드 및 SaaS App 사용 최적화
  - 자체 내장된 기능으로 별도 라이선스 및 장비 없이 사용 가능

- **WAN 보안 강화**
  - 차세대 방화벽 기능(AV, 웹 필터링, IPS 등)를 통해 외부로부터의 위협을 최전선에서 차단
  - SSL 암/복호화 기능으로 모든 트래픽 (HTTP, HTTPS)에 대한 애플리케이션 가시성 및 제어

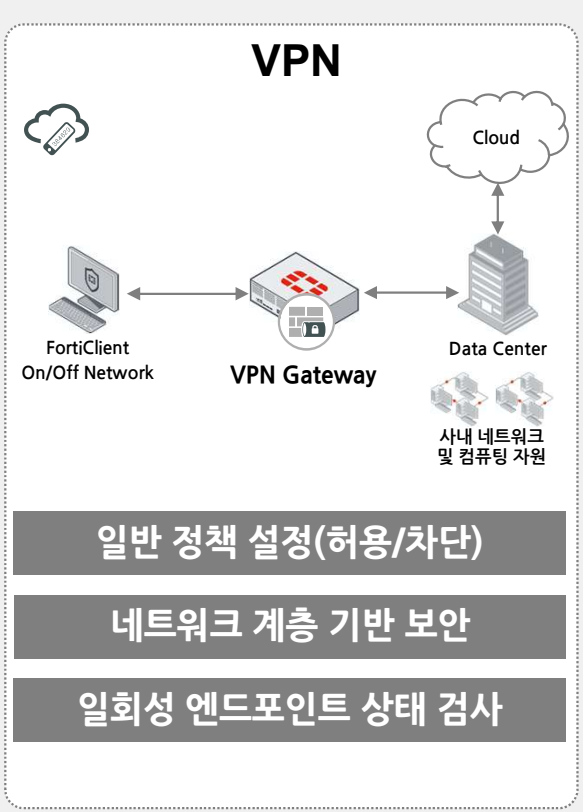


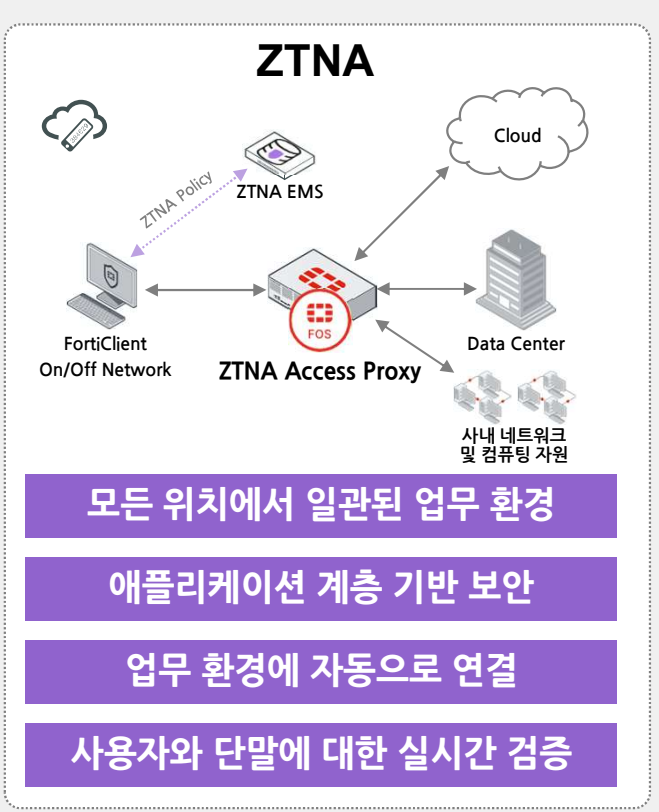
※ 자세한 내용은 FortiGate SD-WAN 소개자료를 추가로 참조하세요

FortiGate - ZTNA Technology

Zero Trust Network Access

- **통상적인 VPN기술의 한계**
  - 기존의 VPN 방식의 네트워크 접근은 **경계 내로 들어가면 네트워크에 광범위하게 엑세스** 할 수 있으며, 클라이언트의 일회성 상태 검사 이후 허용/차단 정책으로 관리
  - 또한 엑세스 위치를 고려하지 않고, 디바이스의 보안상태 체크 없이 사내 망 접근이 가능
- **Fortinet 유니버설 ZTNA 기술**
  - 모든 위치에서 일관된 업무 환경 제공
  - 애플리케이션 계층 기반의 보안 제공
  - 업무 환경에 자동 연결 지원
  - 사용자와 단말에 대한 실시간 검증 지원





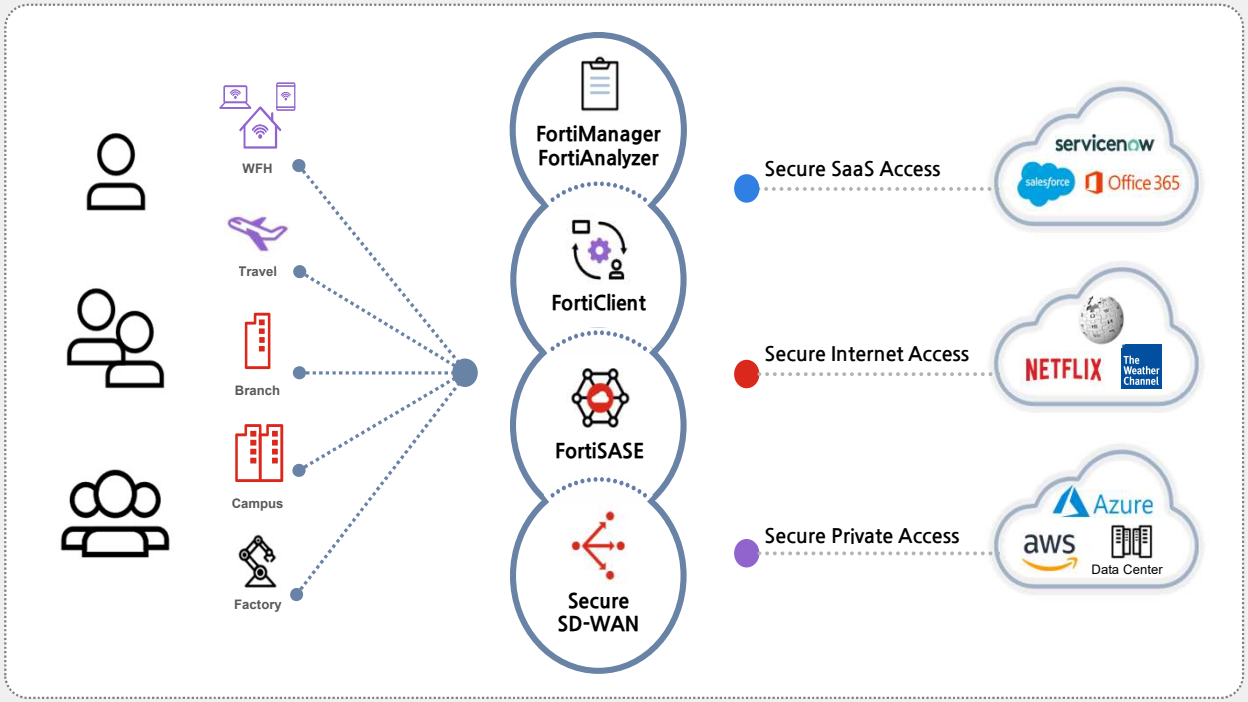
※ 자세한 내용은 Fortinet ZTNA 소개자료를 추가로 참조하세요

FortiGate - Unified SASE

Secure Access Service Edge

- **Fortinet Unified SASE**
  - SASE란 "디지털 비즈니스의 안전한 동적 액세스 요구 사항을 지원하기 위해 포괄적인 네트워크 보안 기능(예: SWG, CASB, FWaaS 및 ZTNA)을 갖춘 전체 WAN 기능"을 제공하는 것
  - NGFW(FWaaS), ZTNA, SD-WAN, SWG, CASB의 솔루션을 모두 제공하는 Fortinet에서 통합된 하나의 온전한 SASE를 제공

- **단일 벤더 SASE의 이점**
  - 운영 단순화 및 비용절감
  - 일관된 보안태세
  - 제품 간의 압도적인 연동성
  - 더 나은 사용자 경험 제공

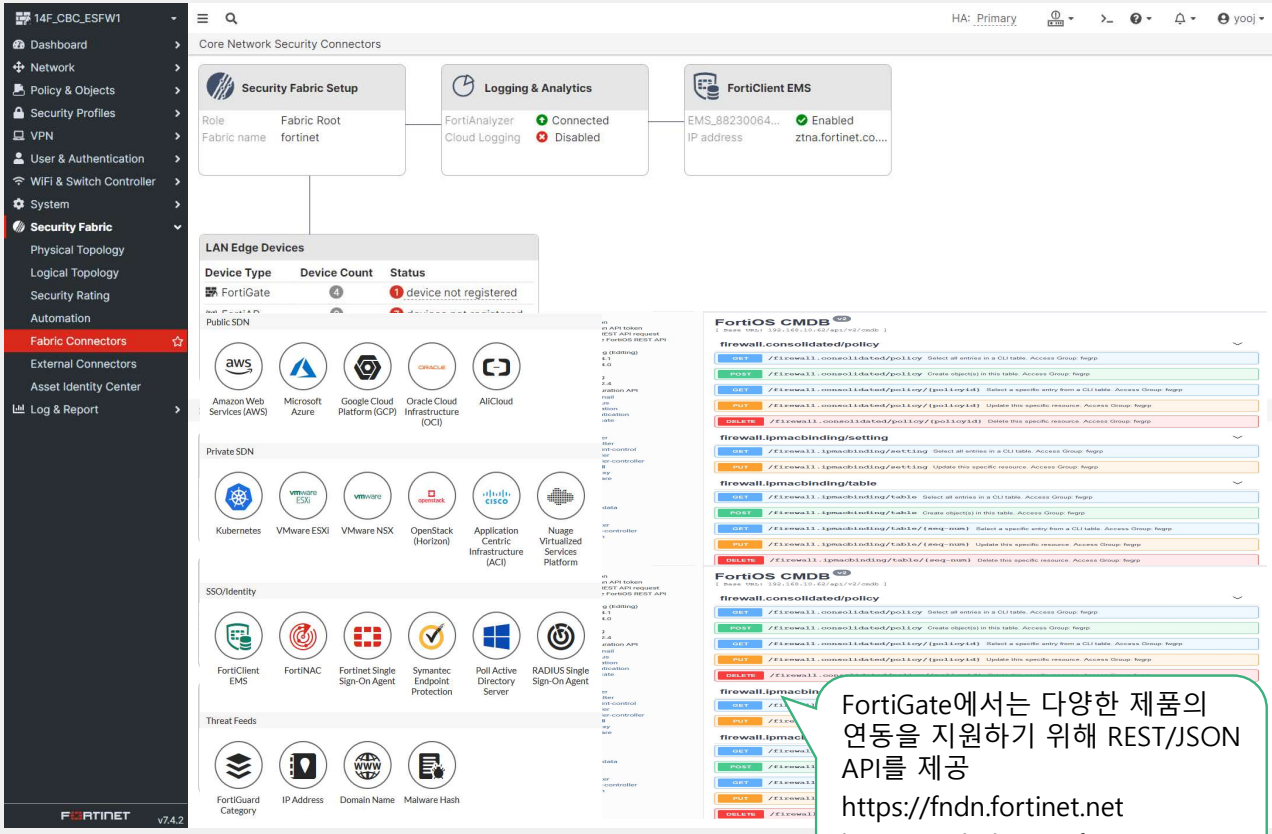


※ 자세한 내용은 Fortinet SASE 소개자료를 추가로 참조하세요

FortiGate Fabric Connector

Fortinet Developer Network – API, Terraform, Ansible 등

- **다양한 플랫폼과의 연동 지원**
  - 최근 애플리케이션과 데이터는 온 프레미스, 프라이빗, 퍼블릭 및 하이브리드 클라우드로 어디서나 배포되고 상주하게 됨
  - DevOps와 클라우드로 인해 운영환경의 변화는 빠르나 **보안 통합 관리에 부담 증가**
  - 패브릭 커넥터를 통해 다양한 클라우드 플랫폼으로부터 보안 정보를 자동 업데이트
  - 또한 클라우드 내부의 리소스 변경이 필요할 경우 API를 통해 **클라우드 Function을 호출** 가능
  - **Threat Feeds 기능**으로 고객사만의 위협 정보를 별도로 관리 가능



FORTINET

Customer Briefing Center
포티넷 CBC 고객 솔루션 체험 센터

전세계 TOP3 사이버 보안 벤더인 포티넷에서 국내 고객 분들을 위해 마련한 솔루션 체험 센터로 방문하시는 고객분들의 요구사항에 따라 맞춤화된 컨설팅을 제공합니다.

보안 중심 네트워크 | 다이나믹 클라우드 보안 | AI 기반 보안 관제 | 제로 트러스트 엑세스

☑ 포티넷CBC에 방문해야 하는 이유?

- 디지털 트랜스포메이션에 필요한 IT보안 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.

포티넷 CBC는 언제나 여러분께 열려있습니다. 지금 방문 신청해주세요!

www.fortinet-vcbc.com www.fortinet.com/kr/corporate/cbc

CBC 방문 신청하기

Virtual CBC 바로가기


FORTINET