



Secure SD-Branch를 통한 비즈니스 네트워크 엣지 보호 구축 사례 및 통합 관리 단순화 방안 소개

포티넷 코리아
이창운 이사



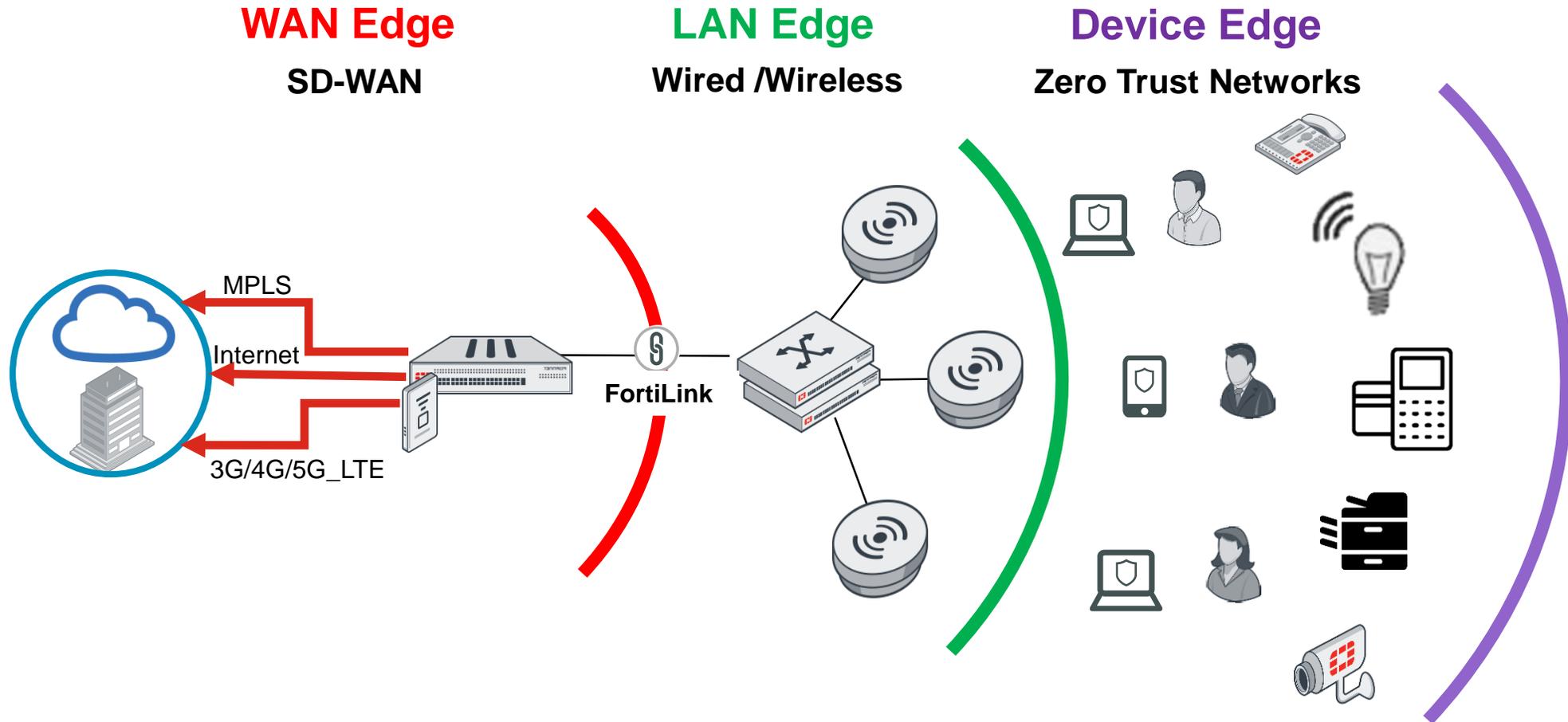
목 차

- 왜 변화가 필요한가?
- 구축 방안으로 본 시큐어 SD-Branch
 - 본사 수준의 네트워크 인프라 보안
 - 보다 간단하고 편리한 통합관리
- 왜 포티넷 시큐어 SD-Branch인가?
 - 포티넷 SD-Branch에 대한 평가
 - 보안을 품은 SD-Branch
 - 이전에 경험하지 못한 네트워크 가시성 등
- 구축사례
- 맺음말

왜 변화가 필요한가?

네트워크 엣지(Edge)란?

NETWORKS EDGE



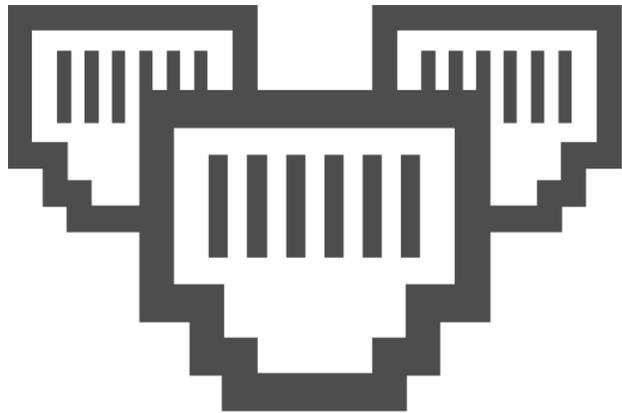
디지털 전환에 따른 비즈니스 계획

WAN 및 LAN 엣지에서 확장

클라우드 진입로

운영의 단순화

IoT 대응



2년 내에 95% 기업이
SD-WAN을 사용

전문기술 부족

310억 개의 디바이스
(2025년에는 750억)

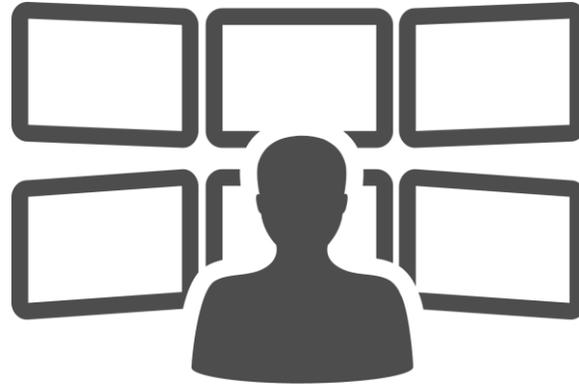
새로운 WAN 및 LAN 엣지 패러다임에 대한 도전과제

이제 각 사용자와 디바이스가 엣지를 대표

보안



복잡



비용



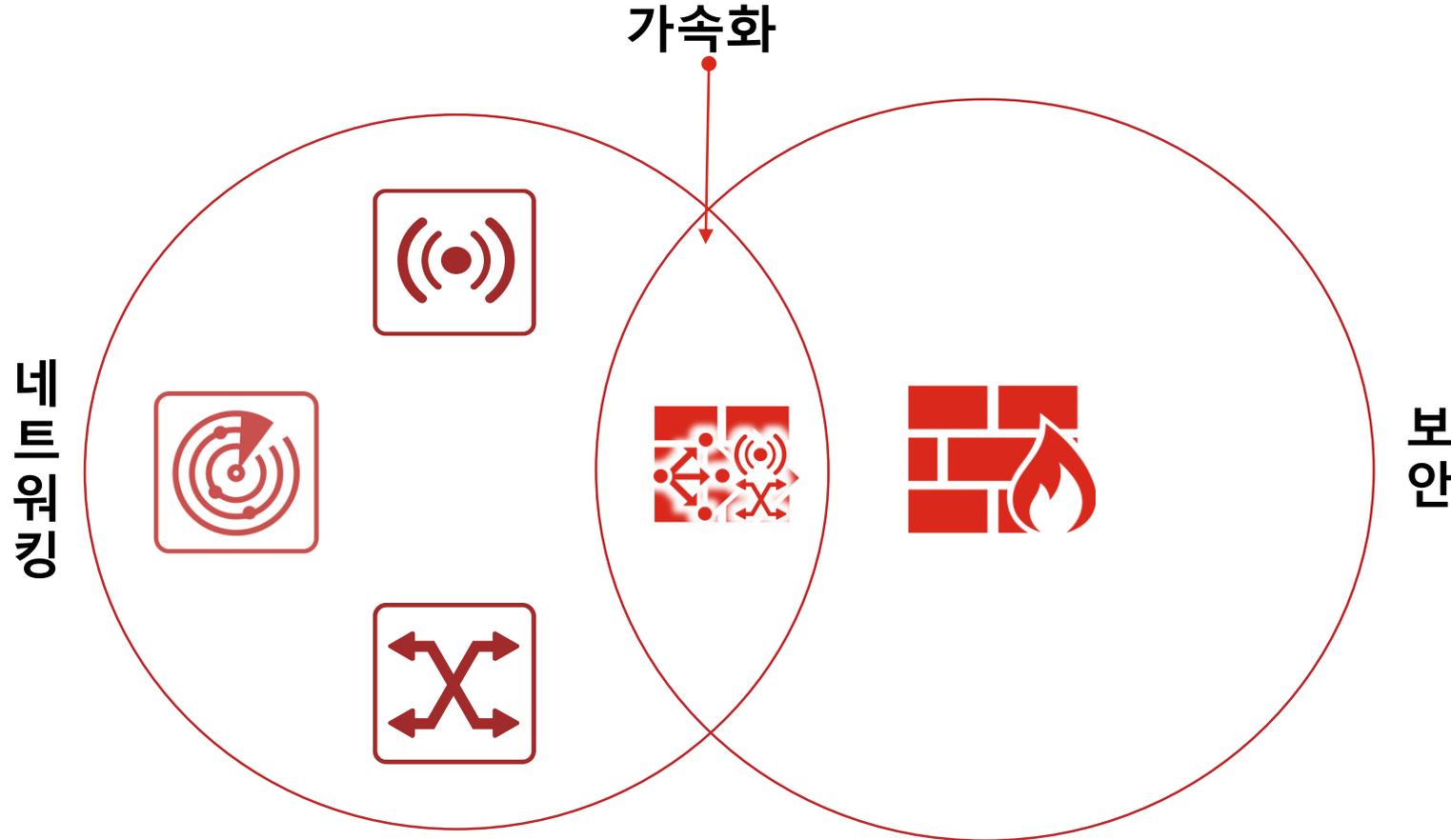
정해져 있는 솔루션

다양한 벤더, 콘솔 및
운영체제

라이선스 및 지원

보안 중심 네트워킹 필요

모든 엣지 및 사용자에게 걸친 네트워킹 및 보안의 통합

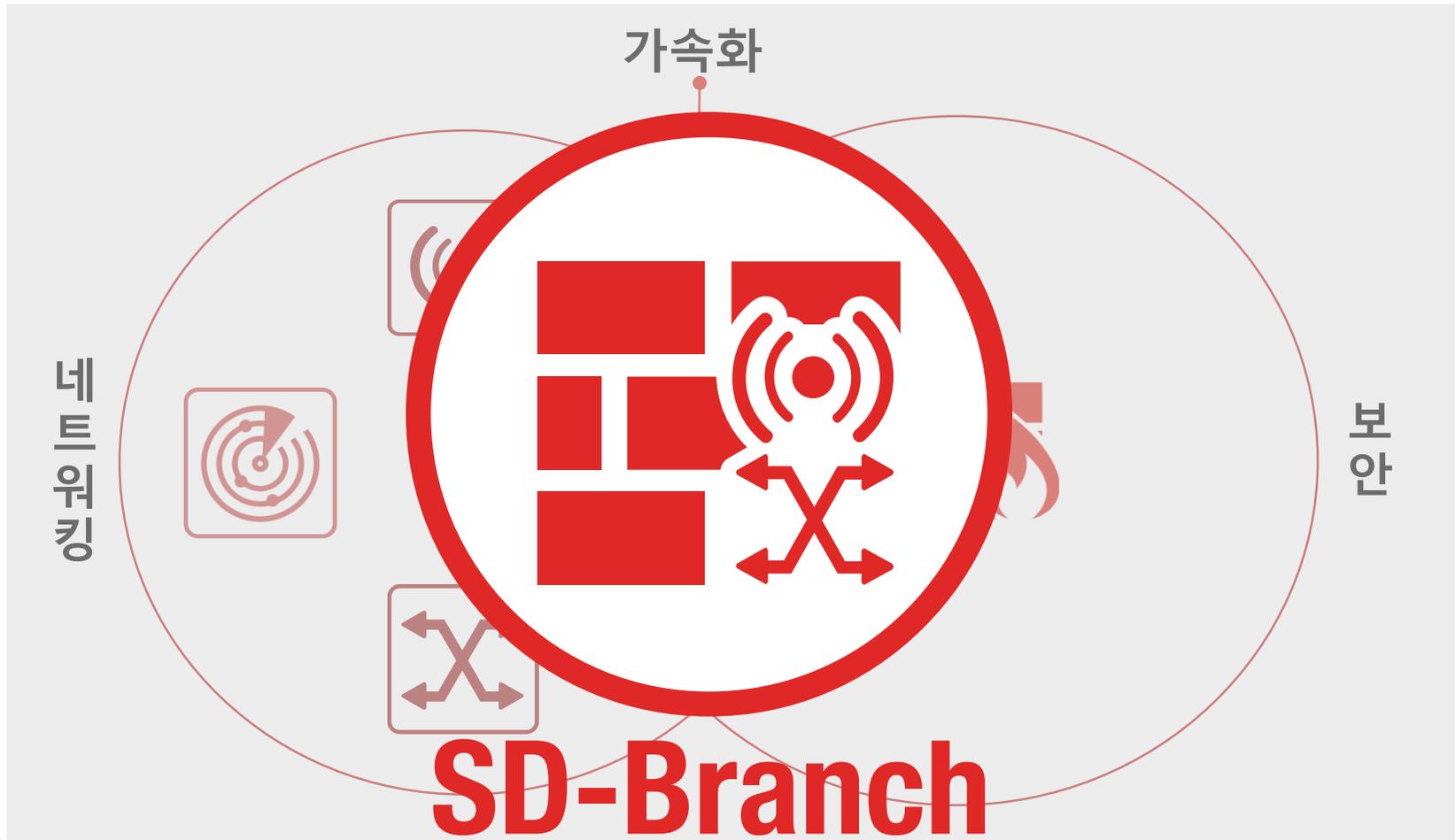


네트워킹 및
보안 통합의
가속화

언제 어디서나 유연하게
보안을 유지

보안 중심 네트워킹 필요

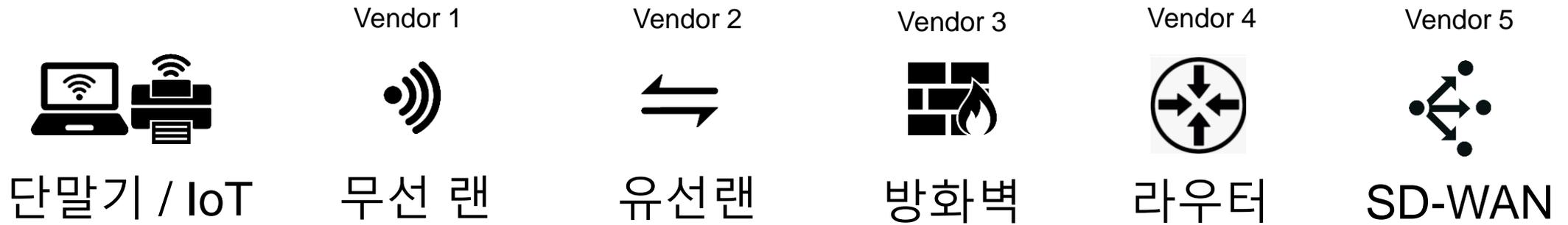
모든 엣지 및 사용자에게 걸친 네트워킹 및 보안의 통합



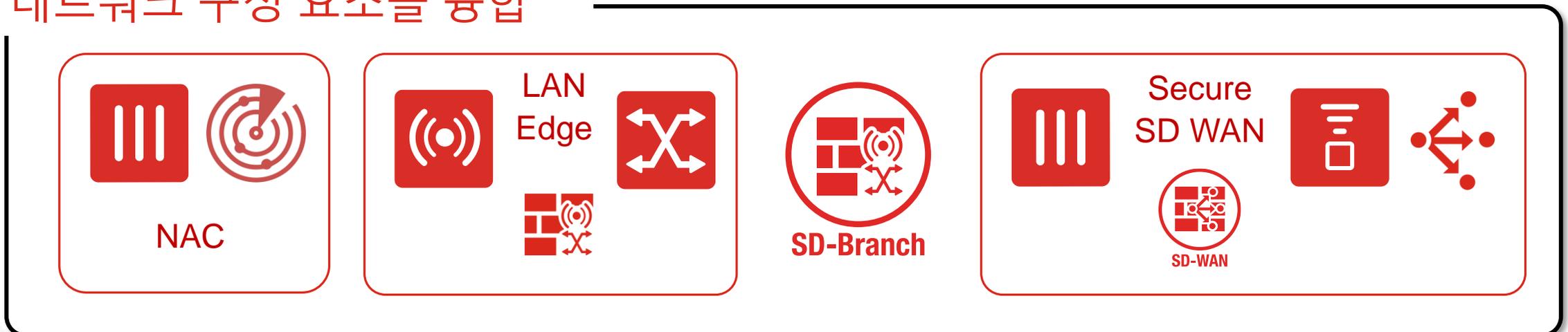
그래서,
SD-Branch가
필요

그래서, SD-Branch가 뭔가요???

전형적인 네트워크 구성 요소



네트워크 구성 요소들 융합



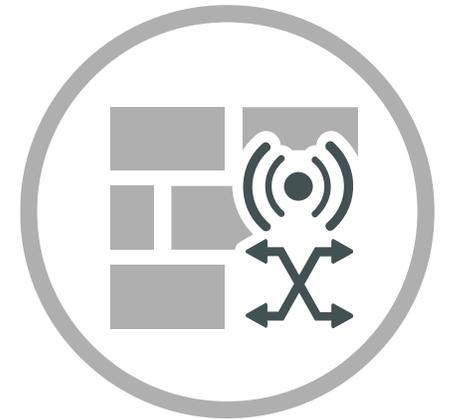
시큐어 SD-Branch

네트워크에 대한 안전하고 민첩한 통합 접근 방식

- 포티넷이 바라보는 성공적인 네트워크 환경을 구축하기 위한 3가지 핵심 요소 :

1. 간단하고
2. 안전하고
3. 비용 효과적인

- 포티넷의 시큐어 SD-Branch 솔루션이 위 요소들을 만족
 - SD-Branch* 관련하여 가트너 매직 쿼드런트 3 개의 항목 모두에서 유일하게 인정받음

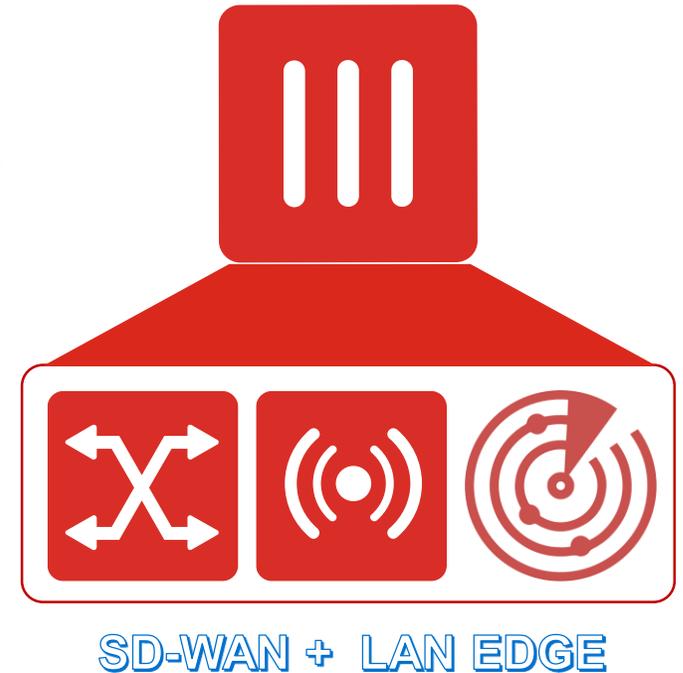


SD-Branch

시큐어 SD-Branch

네트워크에 대한 안전하고 민첩한 통합 접근 방식

- 보안 기반 네트워킹 : 네트워크 액세스와 보안의 융합
- 통합 보안 프레임워크 내에서 네트워크 액세스 레이어 설계.
- 컨버전스 네트워크 환경에 이상적인 차별화된 아키텍처
 - 유연한 확장 제공 : 필요에 따라 네트워크 디바이스를 추가
 - 단순화된 운영, 관리 및 라이선스
 - 전반적으로 소요 비용을 획기적으로 낮춤



포티넷 시큐리티 패브릭

광범위한(BROAD)

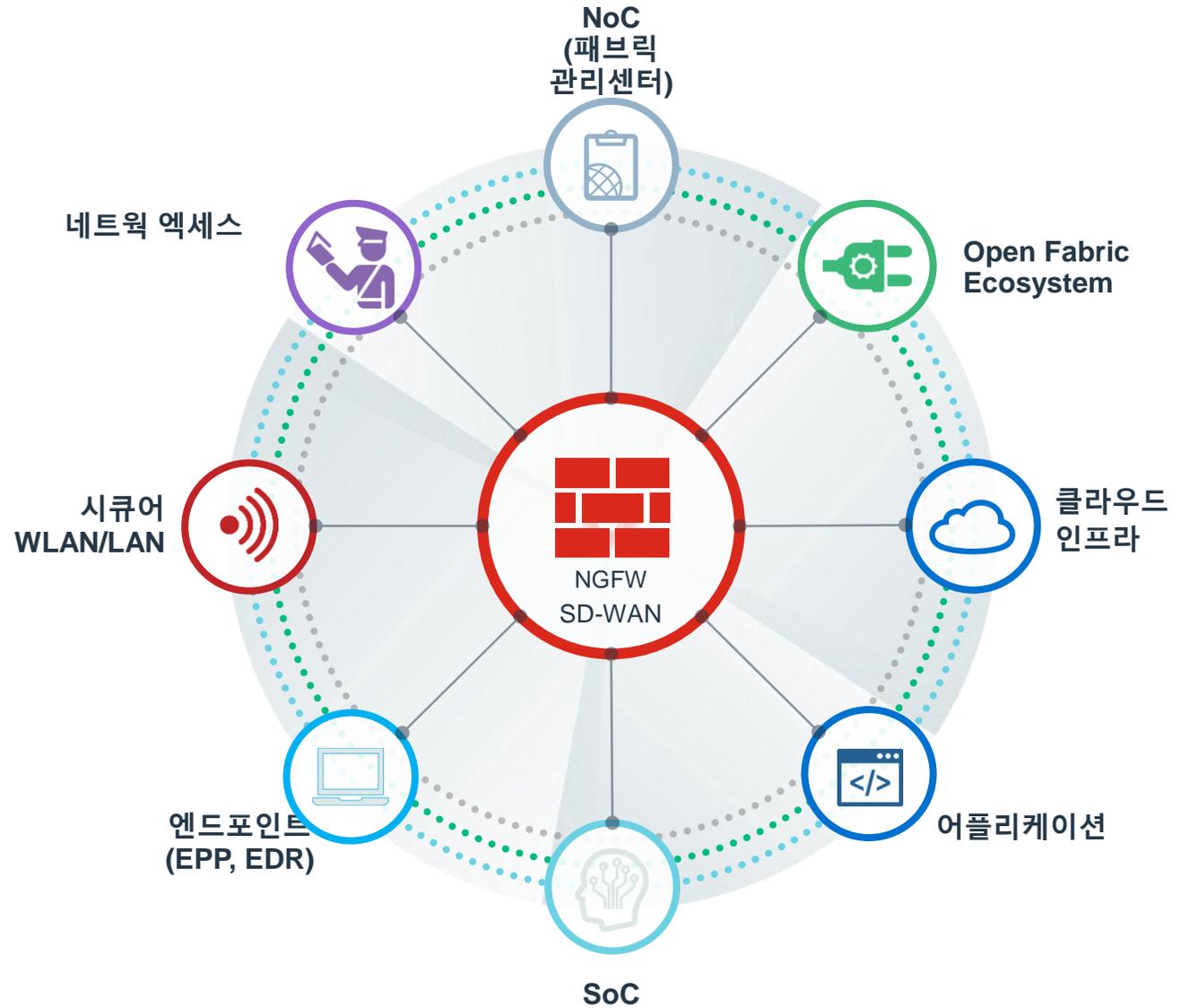
가시성을 기반으로 모든 디지털 공격 영역에 대한 위험을 효과적으로 관리

통합(INTEGRATED)

솔루션으로 여러 개별 제품 지원의 복잡성 감소

자동화된(AUTOIMATED)

워크플로우로 작업 속도와 응답속도를 높임



포티넷 LAN 엣지

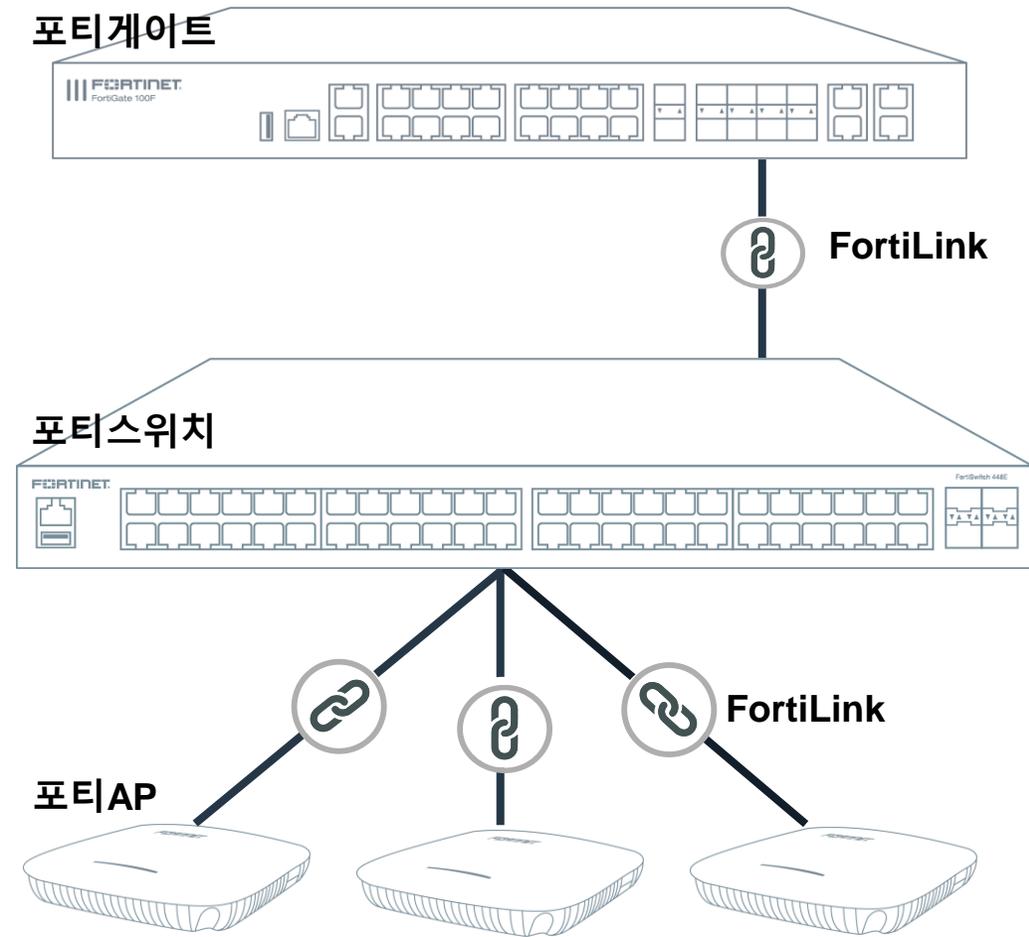
보안 중심 네트워킹

• 통합된 보안

- 포티AP 및 포티스위치를 포티게이트 OS를 통해 직접 제어, 구성 및 관리
- 차세대방화벽의 기능들과 검사를 유선 및 무선 네트워크로 확장
- 중앙집중식 관리를 넘어서는 중요한 단계

• 단순화

- 신속하고 빠르게 구축 및 관리
- 필요한 만큼 언제든지 확장 가능한 유연한 아키텍처
- 낮은 소요 비용
- 포티OS에 포함된 액세스 관리
- 별도의 라이선스가 필요하지 않음

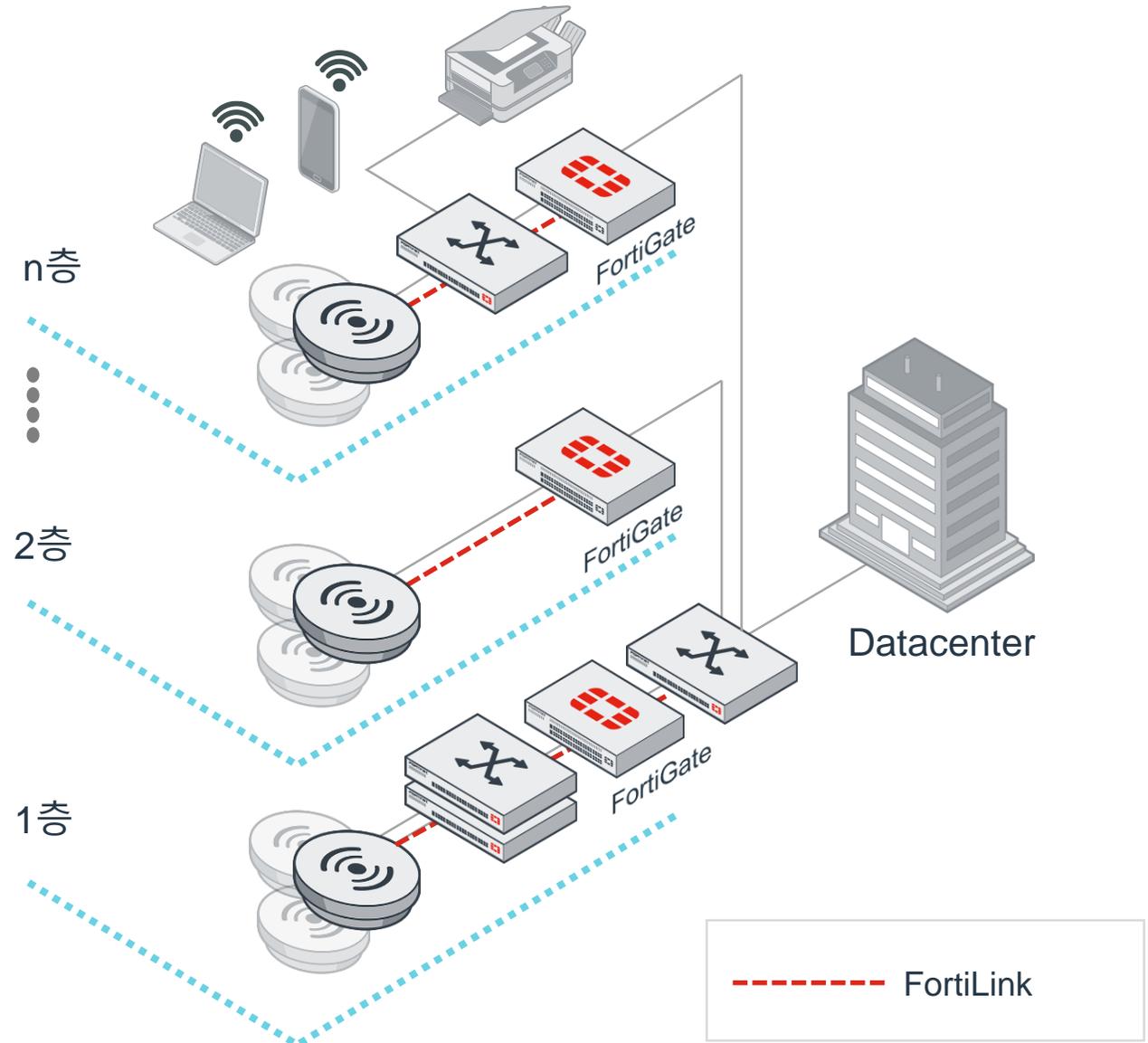


구축 방안으로 본 시큐어 SD-Branch

- 본사 수준의 네트워크 인프라 보안
- 보다 간단하고 편리한 통합관리
- 이전에 경험하지 못한 네트워크 가시성 등

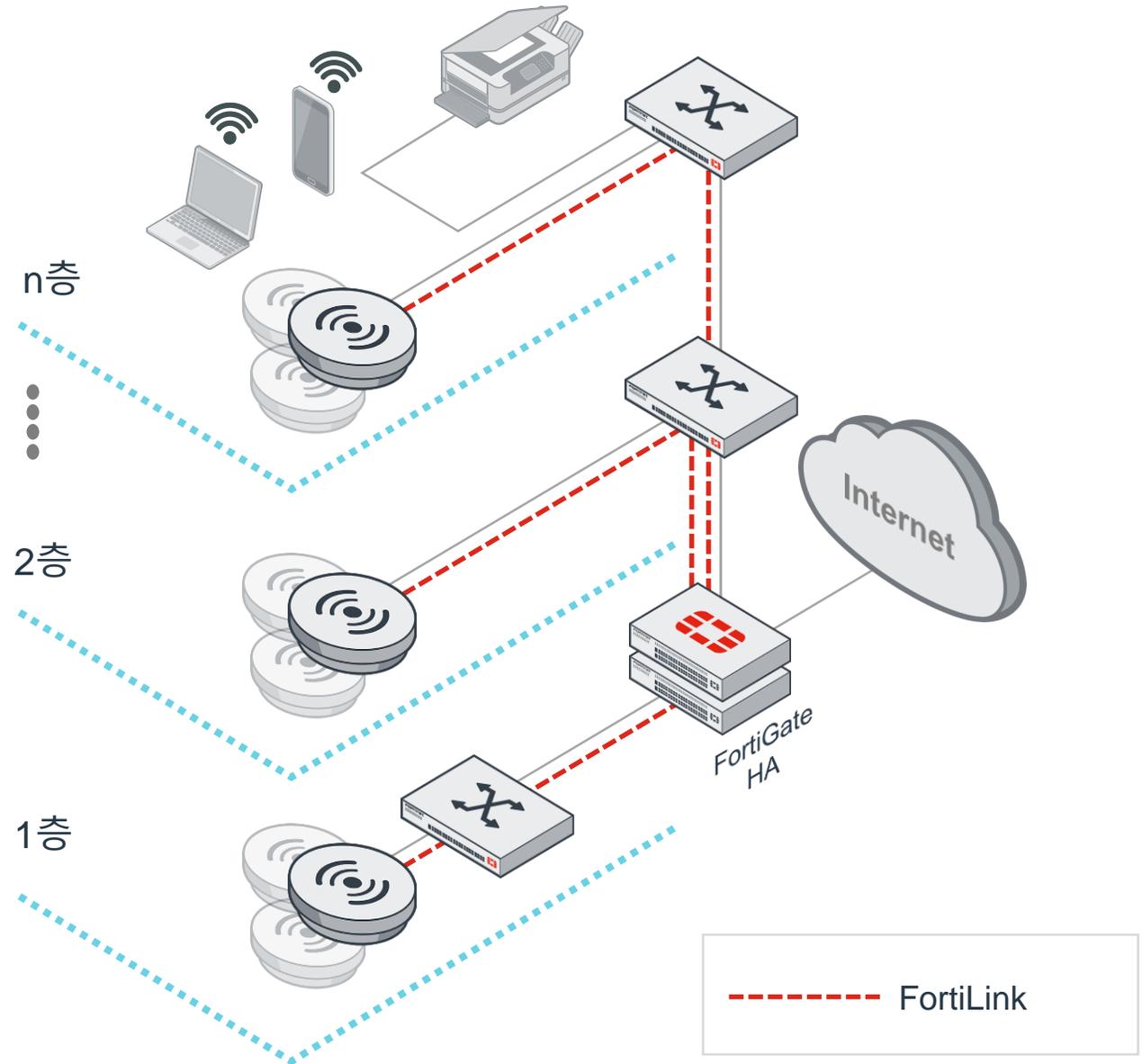
구축방안 : 본사/지사

- 내부 영역을 분리한 포티게이트가 해당 영역의 액세스 계층을 관리
- 데이터 센터에 포티게이트가 추가로 데이터 센터 방화벽으로 존재할 수 있음
- 포티매니저 / 포티아날라이저를 NOC / SOC에서 사용하여 전체 구축 / 제어 / 관리에 대해 단일 창 관리를 제공

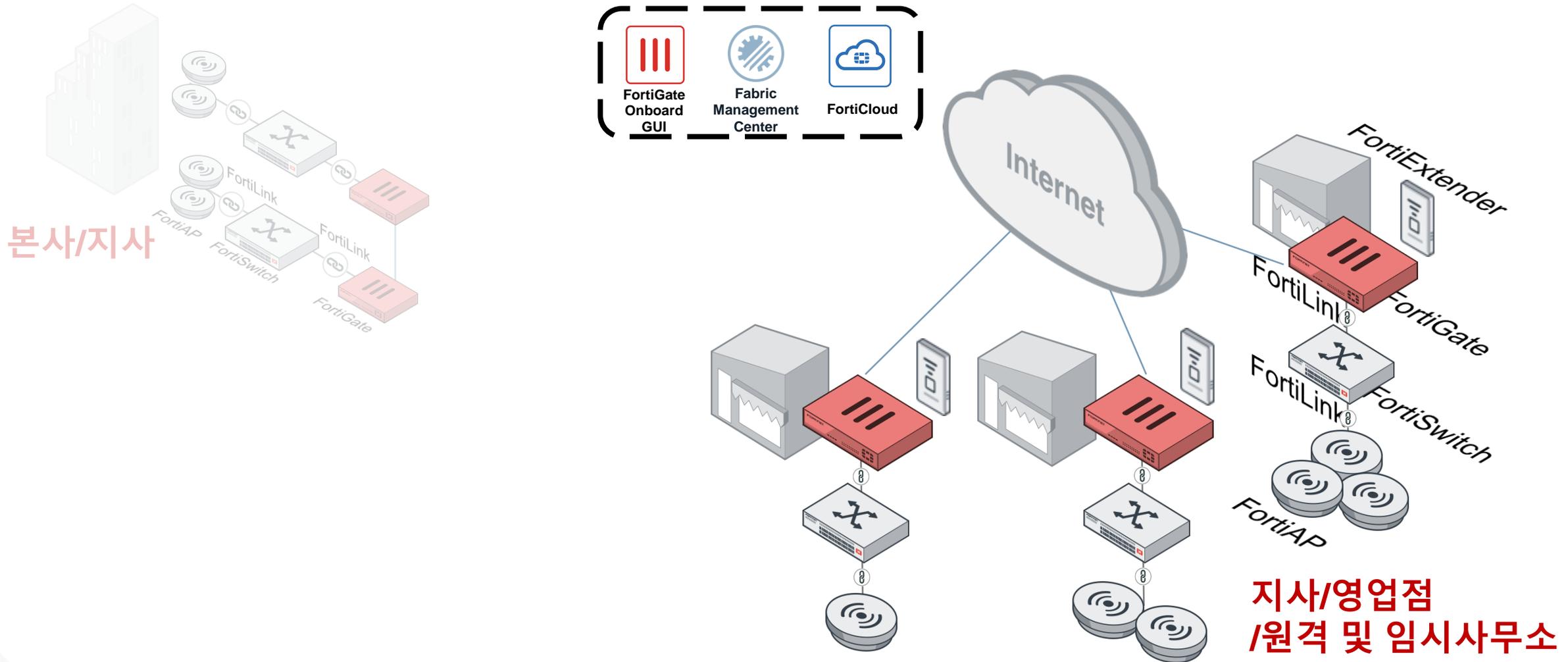


구축방안 : 본사/지사

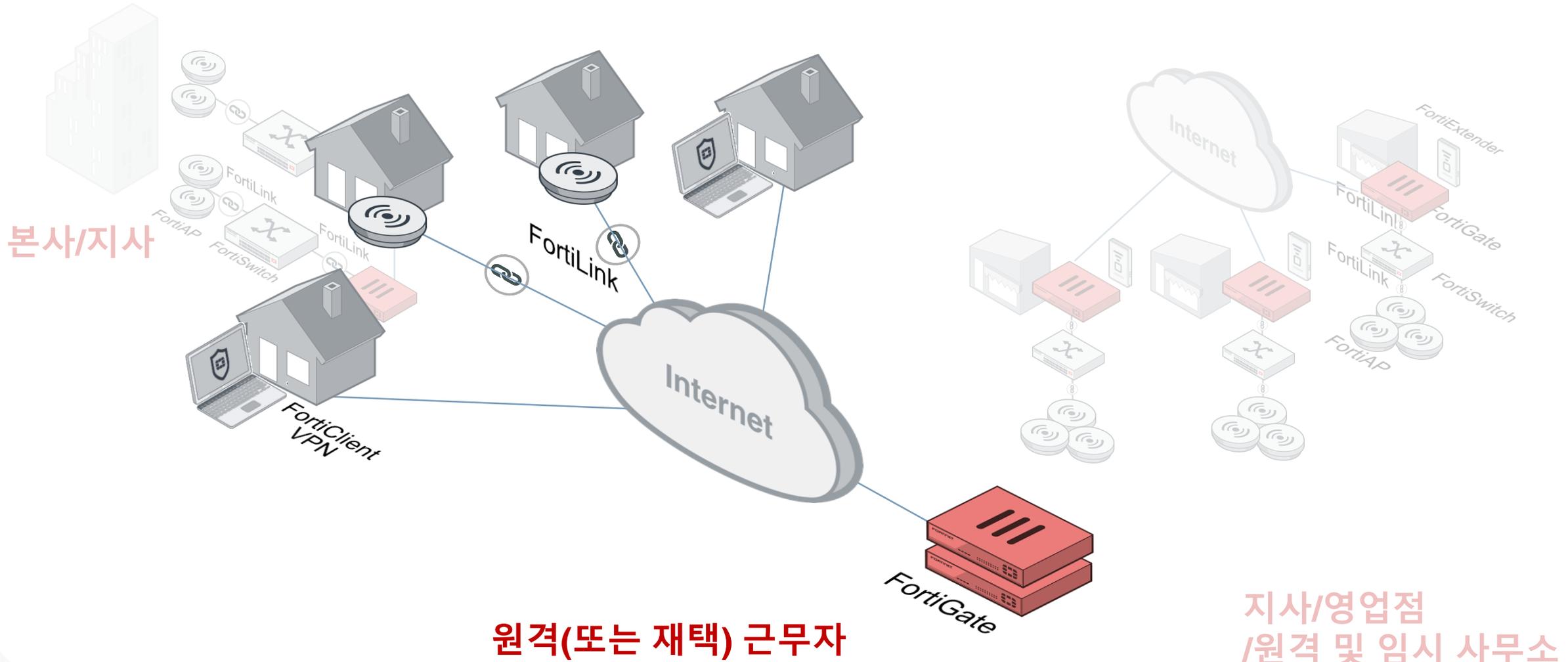
- 포티게이트 이중화 구성을 통해 각 스위치의 2개의 업-링크를 하나로 통합 제어
- 내부 영역을 분리하기 위해 층별 또는 네트워크의 특정 위치에 포티게이트를 추가로 구성할 수도 있음



구축방안 : 지사/영업점/원격 및 임시사무소

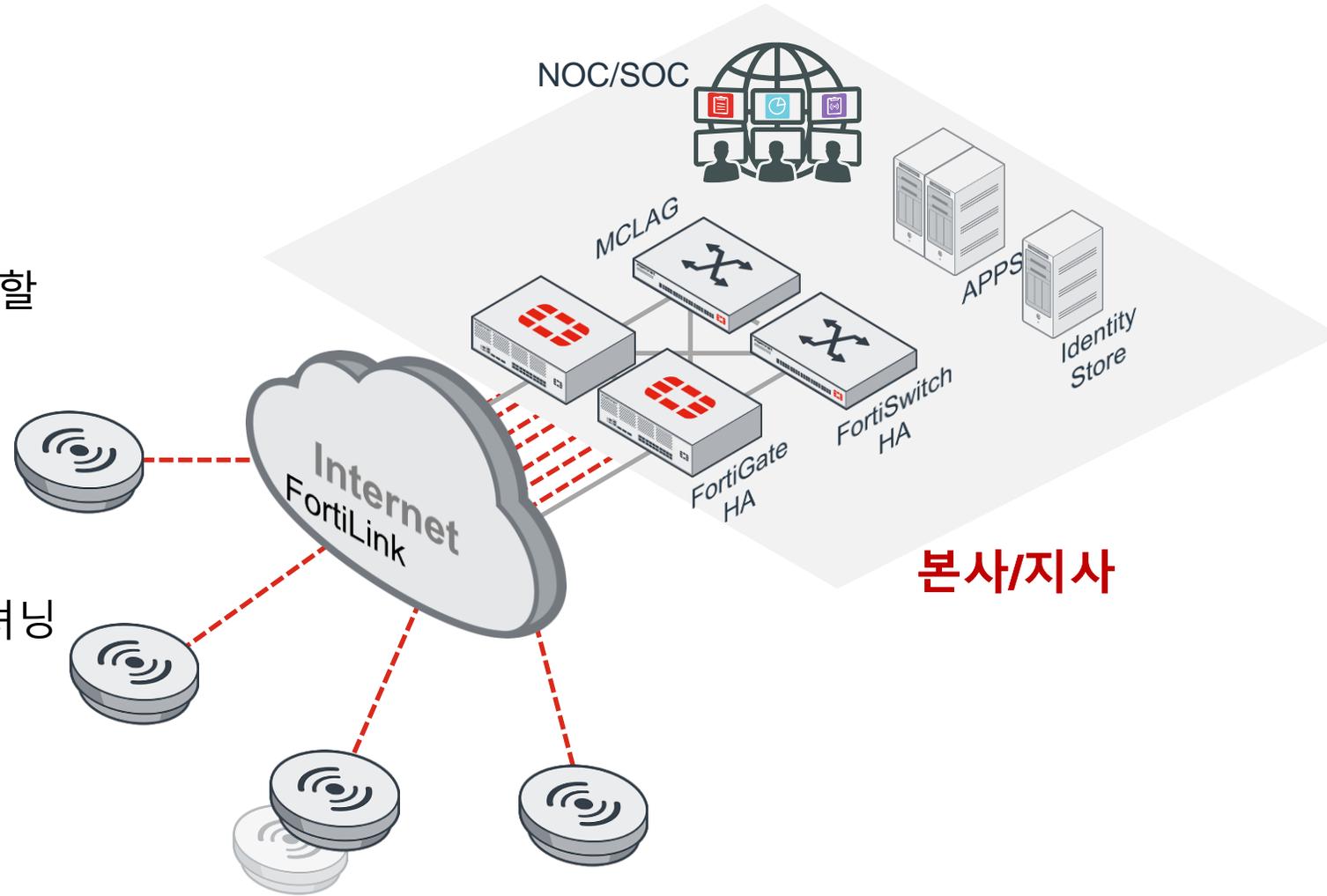


구축방안 : 원격 또는 재택 근무

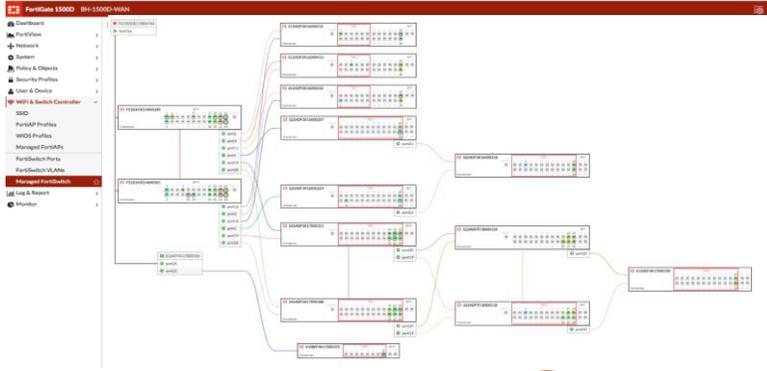


구축방안 : 원격 또는 재택 근무

- 원격 Wi-Fi 네트워킹 구축
 - 모든 포티AP 모델에 적용 가능
 - ✓ 추가 유선 포트가 필요할 경우, 책상 스탠드 액세스서리 등을 선택할 수 있는 벽 부착 모델
 - 포티게이트가 원격으로 관리
 - 포티Deploy를 통한 제로-터치 프로비저닝 제공
 - Split 터널로 비업무 트래픽은 원격지 내부로 처리



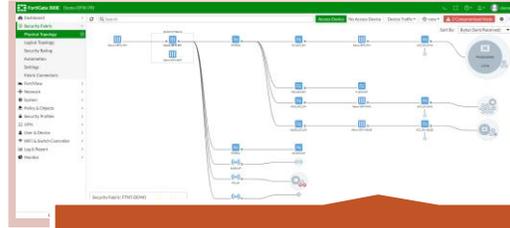
네트워크 가시성 제공



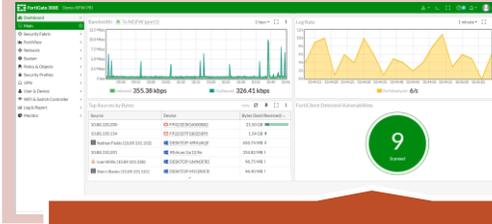
스위치 통합 제어/관리

AP Name	Model	Status	SSID	Channel	Client	OS/Version	IP	MAC	Vendor
12-FP421E-0207-HomeOffice01	FP421E-0207-HomeOffice01	Online	44 F7N1-UEST1 (FTN1-UEST1) 44 F7N1-KORBA (FTN1-WEBSEL1) 44 F7N1-WAVVI (FTN1-WAVVI)	36	1	FP421E-v4.4-bu8R037	192.168.1.10	00:0C:85:64:00:00	Fortinet
12-FP421E-0208-HomeOffice02	FP421E-0208-HomeOffice02	Online	44 F7N1-HEVSI (FTN1-HEVSI) 44 F7N1-UEST1 (FTN1-UEST1) 44 F7N1-KORBA (FTN1-WEBSEL1) 44 F7N1-WAVVI (FTN1-WAVVI)	44	2	FP421E-v4.4-bu8R037	192.168.1.11	00:0C:85:64:00:00	Fortinet
12-FP421E-0209-StrongHome01	FP421E-0209-StrongHome01	Online	44 F7N1-UEST1 (FTN1-UEST1) 44 F7N1-KORBA (FTN1-WEBSEL1) 44 F7N1-WAVVI (FTN1-WAVVI)	36	2	FP421E-v4.4-bu8R037	192.168.1.12	00:0C:85:64:00:00	Fortinet
12-FP421E-0208-Locke01	FP421E-0208-Locke01	Online	44 F7N1-UEST1 (FTN1-UEST1) 44 F7N1-KORBA (FTN1-WEBSEL1) 44 F7N1-WAVVI (FTN1-WAVVI)	36	14	FP421E-v4.4-bu8R037	192.168.1.13	00:0C:85:64:00:00	Fortinet
12-FP421E-0201-SeaView01	FP421E-0201-SeaView01	Online	44 F7N1-UEST1 (FTN1-UEST1) 44 F7N1-KORBA (FTN1-WEBSEL1) 44 F7N1-WAVVI (FTN1-WAVVI)	36	3	FP421E-v4.4-bu8R037	192.168.1.14	00:0C:85:64:00:00	Fortinet
12-FP421E-0203-CBC01	FP421E-0203-CBC01	Online	44 F7N1-UEST1 (FTN1-UEST1) 44 F7N1-KORBA (FTN1-WEBSEL1) 44 F7N1-WAVVI (FTN1-WAVVI)	36	0	FP421E-v4.4-bu8R037	192.168.1.15	00:0C:85:64:00:00	Fortinet
12-WPA-140131-BERC_Park	WPA-140131-BERC_Park	Online	44 F7N1-UEST1 (FTN1-UEST1) 44 F7N1-KORBA (FTN1-WEBSEL1) 44 F7N1-WAVVI (FTN1-WAVVI)	36	1	FP421E-v4.4-bu8R037	192.168.1.16	00:0C:85:64:00:00	Fortinet

AP 통합 제어/관리



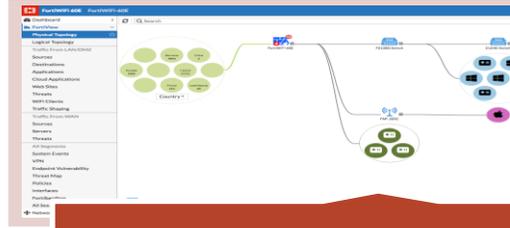
연결 위치



네트워크 사용량

Source	Destination	Protocol	Application	Priority	Result
192.168.1.10	192.168.1.11	TCP	HTTP	High	Success
192.168.1.10	192.168.1.12	TCP	HTTP	High	Success
192.168.1.10	192.168.1.13	TCP	HTTP	High	Success
192.168.1.10	192.168.1.14	TCP	HTTP	High	Success
192.168.1.10	192.168.1.15	TCP	HTTP	High	Success
192.168.1.10	192.168.1.16	TCP	HTTP	High	Success

트래픽 종류



디바이스 종류



맥어드레스

Application	Usage	Priority	Result
Internet Explorer	High	Success	
Microsoft Word	High	Success	
Microsoft Excel	High	Success	
Microsoft PowerPoint	High	Success	
Microsoft Access	High	Success	
Microsoft Outlook	High	Success	

어플리케이션



보안 위협

Event	Source	Destination	Action	Result
Denial of Service	192.168.1.10	192.168.1.11	Blocked	Success
Malware	192.168.1.10	192.168.1.11	Quarantined	Success
Phishing	192.168.1.10	192.168.1.11	Blocked	Success
Spam	192.168.1.10	192.168.1.11	Blocked	Success
Malicious URL	192.168.1.10	192.168.1.11	Blocked	Success

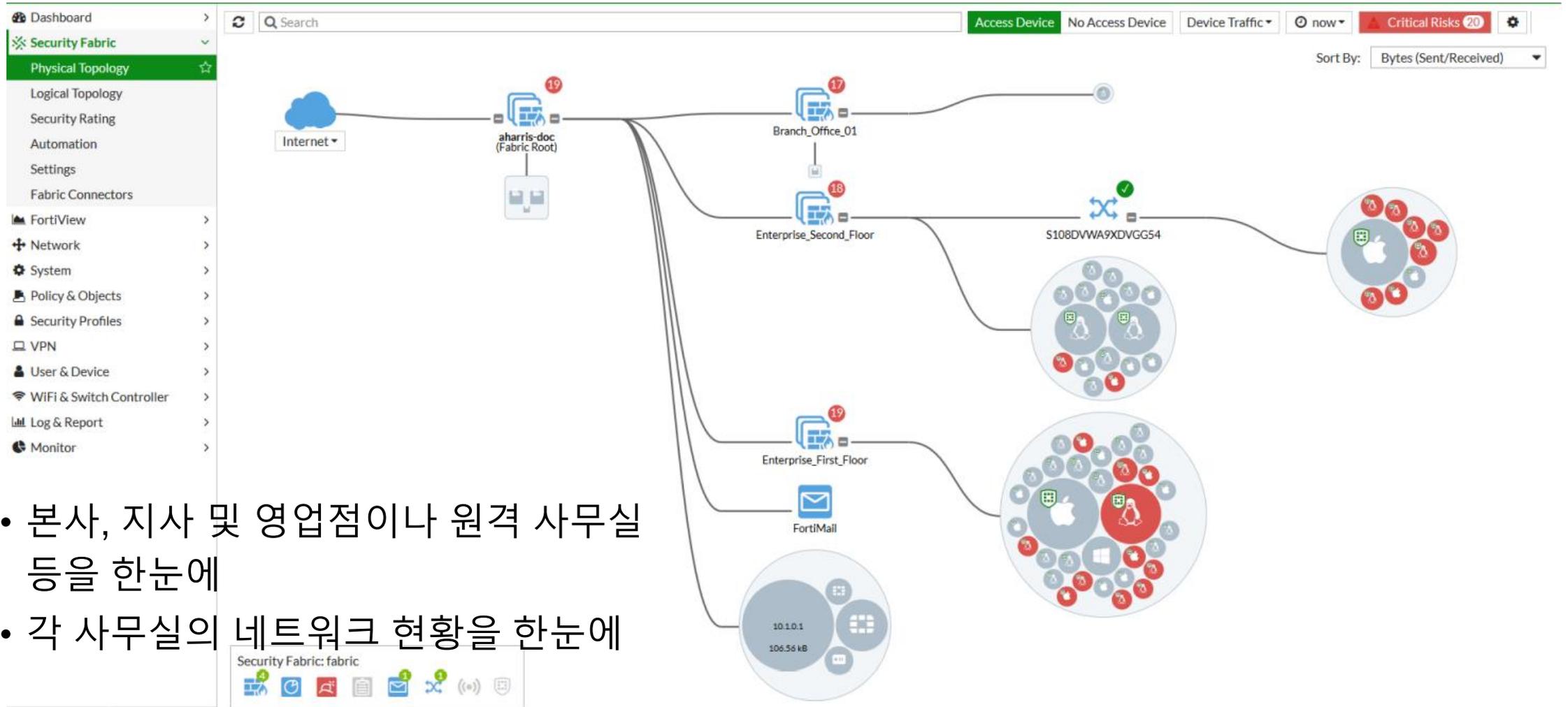
취한 조치

Item	Value	Unit
AP Uptime	100%	%
AP CPU Usage	10%	%
AP Memory Usage	50%	%
AP Disk Usage	20%	%
AP Temperature	45°C	°C
AP Power	10W	W

준수사항

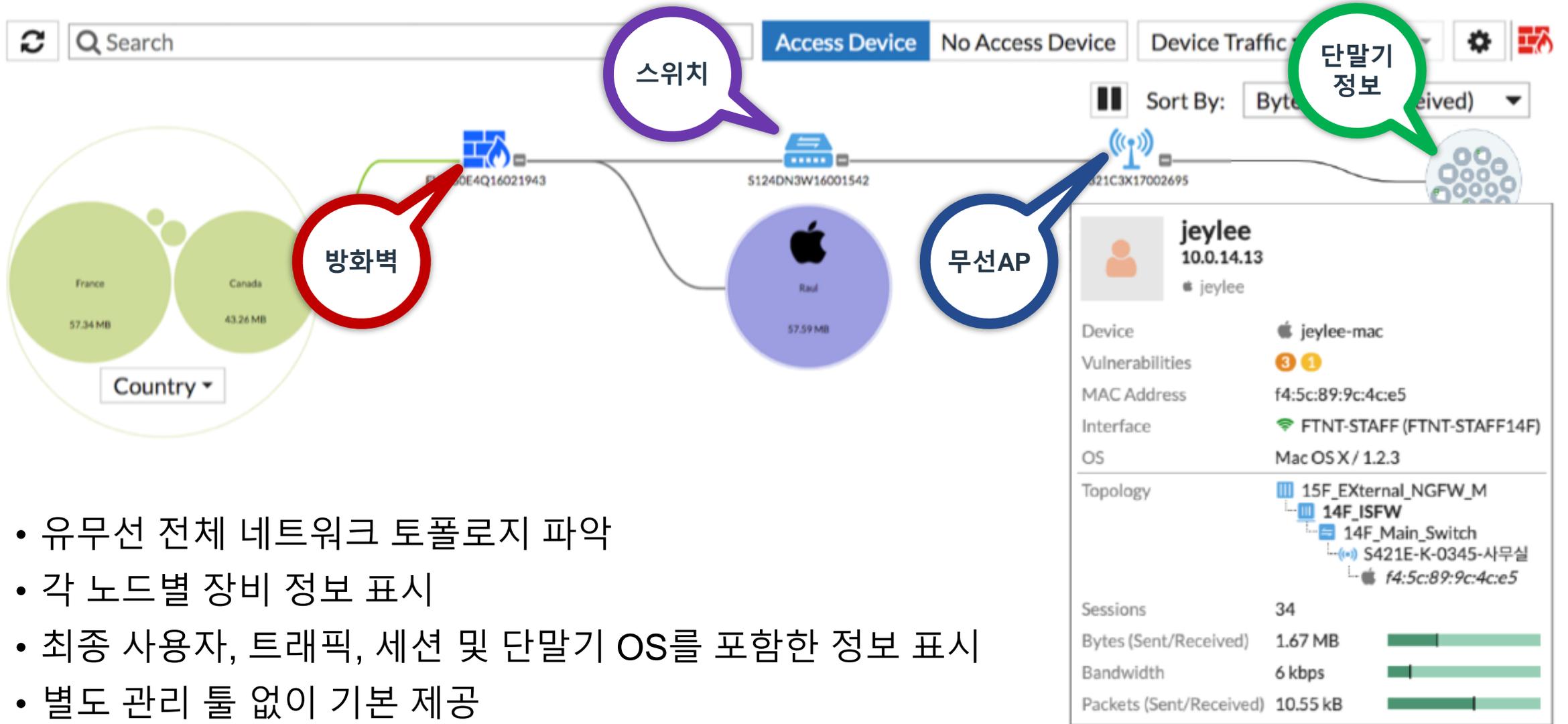
연결 단계에서 어플리케이션 및 보안까지 모든 것을 볼 수 있음

네트워크 가시성 제공



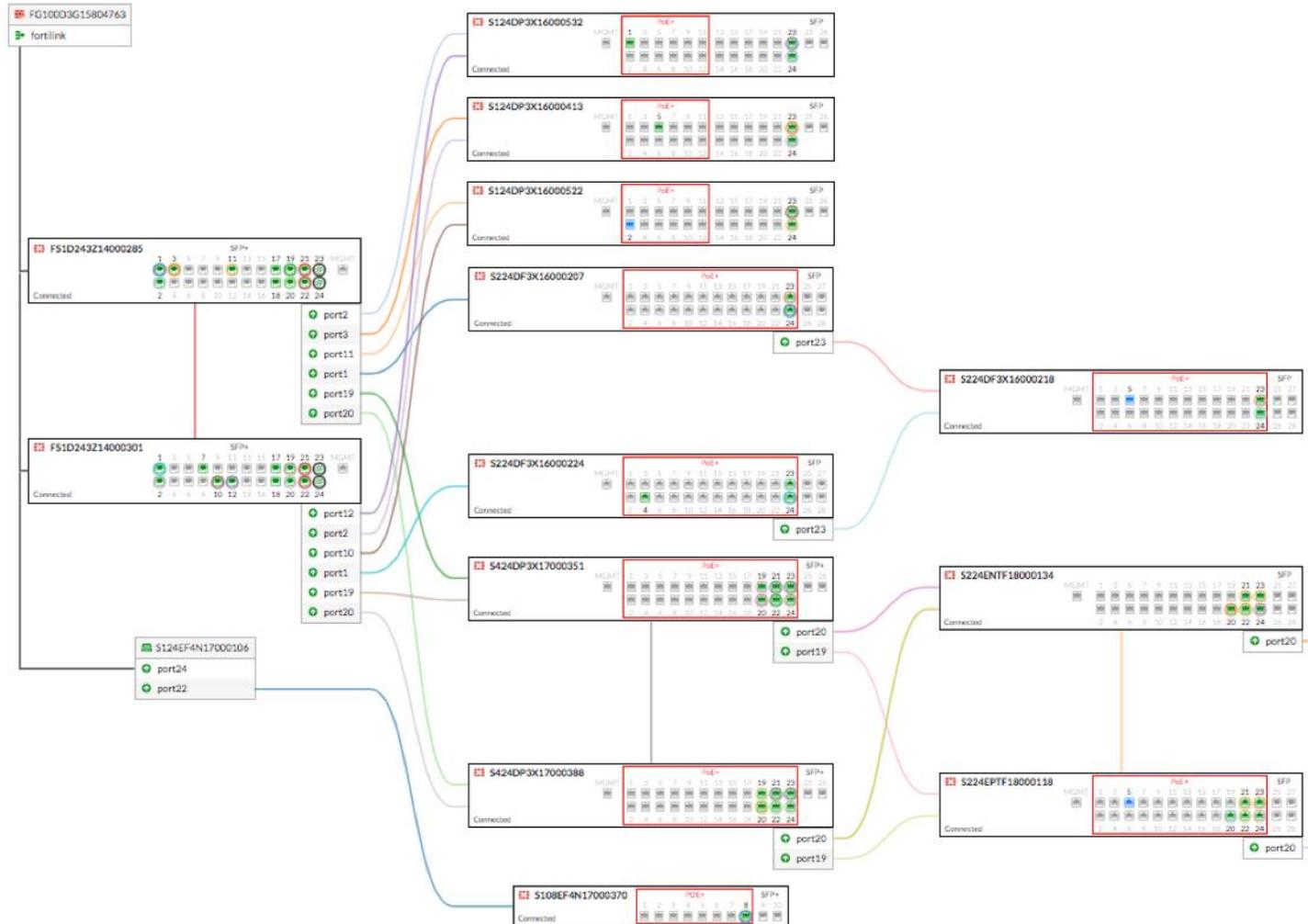
- 본사, 지사 및 영업점이나 원격 사무실 등을 한눈에
- 각 사무실의 네트워크 현황을 한눈에

네트워크 가시성 제공



- 유무선 전체 네트워크 토폴로지 파악
- 각 노드별 장비 정보 표시
- 최종 사용자, 트래픽, 세션 및 단말기 OS를 포함한 정보 표시
- 별도 관리 툴 없이 기본 제공

네트워크 가시성 제공



- 이전에 보지 못한 스위치의 연결성 등 표시
- 스위치간 연결에 대한 정보 및 포트 별로 다른 색으로 정의
- 네트워크 장비 연결 정보를 보다 쉽게 이해할 수 있도록 도와줌
- 이 모든 작업을 위해 별도로 관리자의 설정 등이 필요하지 않고, 자동인식

네트워크 가시성 제공

The interface displays a central hub connected to several wireless APs. Each AP is represented by a circular icon with a signal strength indicator. The APs are:

- SS548DF4K16000195
- SS548DF4K16000200
- PS421E-0239-카페테리아
- PS421E-0268-사무실창측
- PS421E-0301-서올룸옆

Below the AP icons is a table with the following columns: Access Point, Status, Connected Via, and SSIDs.

Access Point	Status	Connected Via	SSIDs
FP421E3X17002257	Online	172.16.14.20 - To-15F-Ext-FW (port40)	Radio 1: FTNT- Radio 2: FTNT-
FP421E3X17002265	Online	172.16.14.24 - To-15F-Ext-FW (port40)	Radio 1: FTNT- Radio 2: FTNT-
PS421E-0239-카페테리아@15F	Online	172.16.15.19 - vsw.port39	Radio 1: FTNT- Radio 2: FTNT-
PS421E-0268-사무실창측@15F	Online	172.16.15.22 - vsw.port39	Radio 1: FTNT- Radio 2: FTNT-
PS421E-0301-서올룸옆@15F	Online	172.16.15.28 - vsw.port39	Radio 1: FTNT- Radio 2: FTNT-

Overlaid on the interface are two detailed health status windows for APs PS421E-0268-사무실창측@15F and PS421E-0239-카페테리아@15F. These windows show general health (Poor), 2.4 GHz health (Fair), and 5 GHz health (Good) metrics, including CPU usage, memory usage, and connection uptime. A table at the bottom of these windows lists connected clients with their SSIDs, device names, channels, bandwidth, and signal strength.

At the bottom of the interface is a floor plan showing the physical layout of the building with AP locations marked as AP01 through AP13.

- 이전에 보지 못한 무선 AP의 연결성 표시
- 각 무선 AP 연결 정보를 보다 쉽게 이해할 수 있도록 도와줌
- 각 무선 AP는 관리자의 설정 등이 필요하지 않고, 자동인식

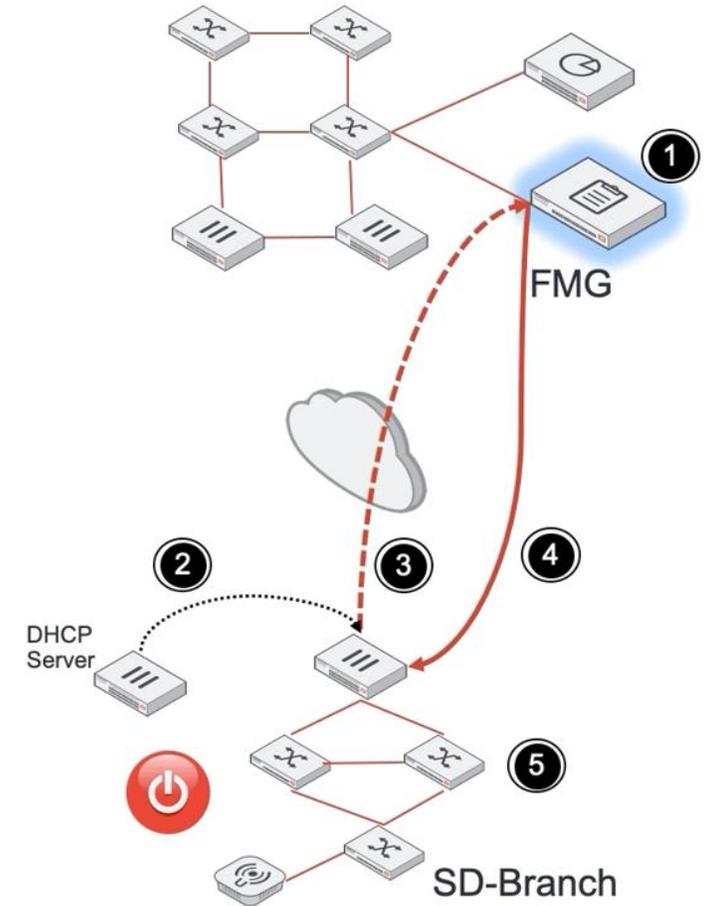
비인가 기기들이 네트워크에 연결되는 것을 방지

- 네트워크 연결 보안을 위한 정책 수행 고려:
 - 회사 기기 및 사용자에게 인증
 - 기기 MAC 주소*를 기반으로 헤드리스 기기 인증
 - 사용자 또는 그룹 별 접근 정책
- 인증되지 않았거나 비인가 기기의 경우:
 - 별도의 세그먼트로 구성
 - 연결 및 대역폭 사용 제한
 - SD-WAN에 트래픽 최적화 시키지 않음
- NAC 솔루션 연동
 - 디바이스 프로파일링으로 좀 더 세부적인 규칙 적용 등

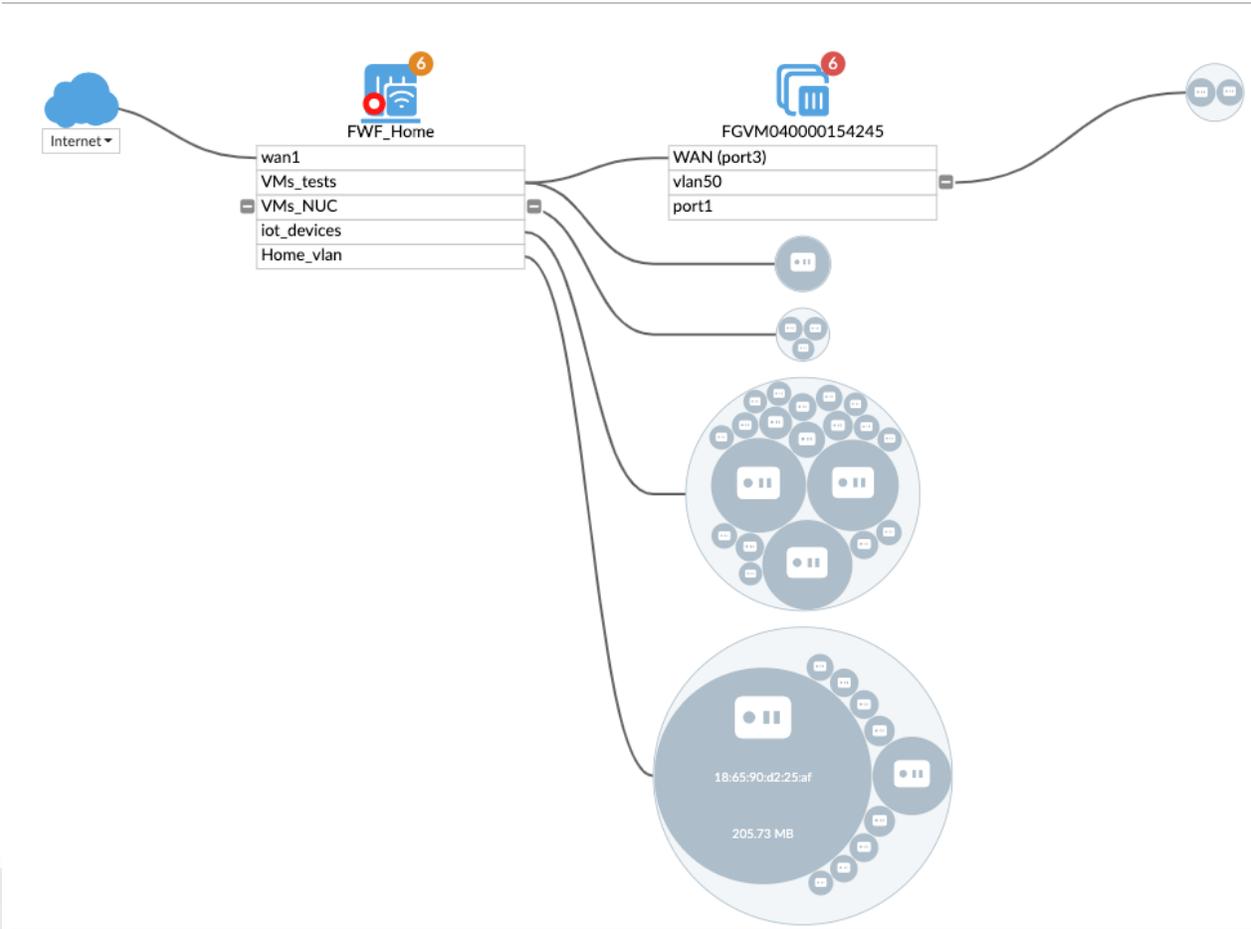


제로 터치를 통한 쉬운 구축

- 배송, 연결하고 잠시 대기
- 다양한 자동화 수준
 - 완전 자동화 (DevOps 또는 DevSecOps)
 - 의사 자동화:
 - ✓ 모델 장비 기반
 - ✓ 또는 템플릿 기반
- SD-Branch 구축을 위해 현장에 전문 인력이나 별도 기술 인력이 필요하지 않음
 - 장비를 배송
 - 전원 및 케이블 연결을 위한 기본 설명서 배포
 - 원격으로 IT 팀 또는 담당자가 작업을 수행



Single Pane of Glass로 관리 포인트의 일원화



SD-WAN 네트워크

- 포티게이트
- SLA
- 회선 상태
- 어플리케이션

SD-BRANCH 네트워크

- 포티게이트
- 포티스위치, 포티AP
- NAC : NAC Lite, FNAC

디바이스

- OS
- MAC 및 IP 주소
- 사용자
- 트래픽

왜 포티넷 시큐어 SD-Branch인가?

- 포티넷 시큐어 SD-Branch솔루션에 대한 평가

시장 조사 기관에서 바라보는 포티넷 솔루션

2020 Magic Quadrant for Network Firewalls

Figure 1. Magic Quadrant for Network Firewalls



Source: Gartner (November 2020)

Fortinet Recognized as a Leader

2020 was 10th time in a row that Fortinet is in the Gartner Magic Quadrant for Network Firewalls

2020 Magic Quadrant for WAN Edge Infrastructure

Figure 1. Magic Quadrant for WAN Edge Infrastructure



Source: Gartner (September 2020)

Fortinet Recognized as a Leader

With Higher Ability to Execute and Further Completeness of Vision Than the Previous Year

2020 Magic Quadrant for Wired and Wireless LAN Infrastructure

Figure 1. Magic Quadrant for Wired and Wireless LAN Access Infrastructure

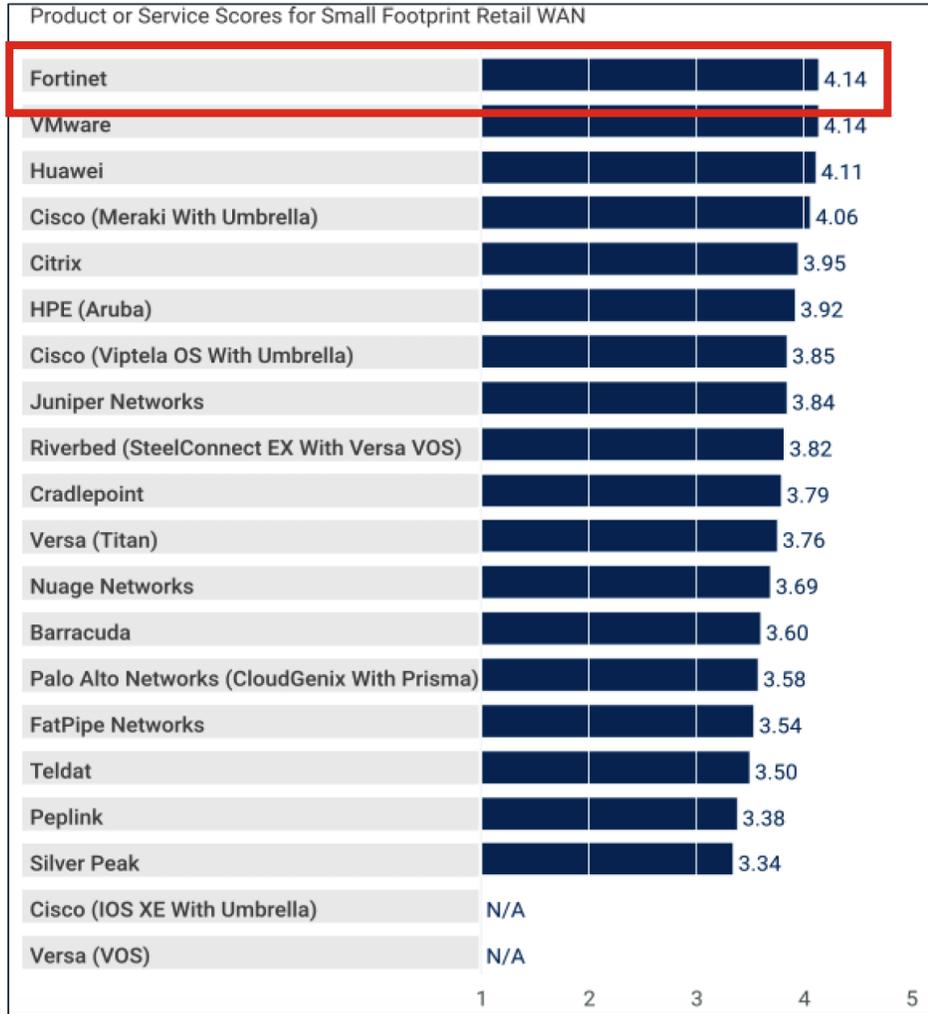


2020 Gartner Magic Quadrant for Wired/Wireless LAN Access Infrastructure

Security-driven Networking – the Definition of Visionary

Fortinet's Security-driven Networking strategy delivers a unique and differentiated approach to the market. They offer customers increased features without the need for licenses

고객들이 평가하는 포티넷 솔루션



These graphics were published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner documents are available upon request from our website: <https://www.fortinet.com/solutions/gartner-magic-quadrants.html>.

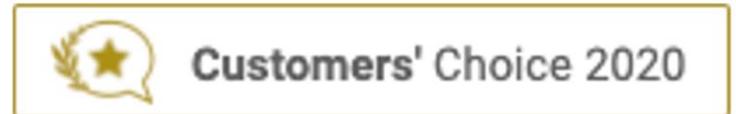


The Customers Have Spoken

Gartner Peer Insights Customers' Choice distinctions recognize vendors and products that are highly rated by their customers. The data we've collected represents a top-level synthesis of vendor software products most valued by IT Enterprise professionals.

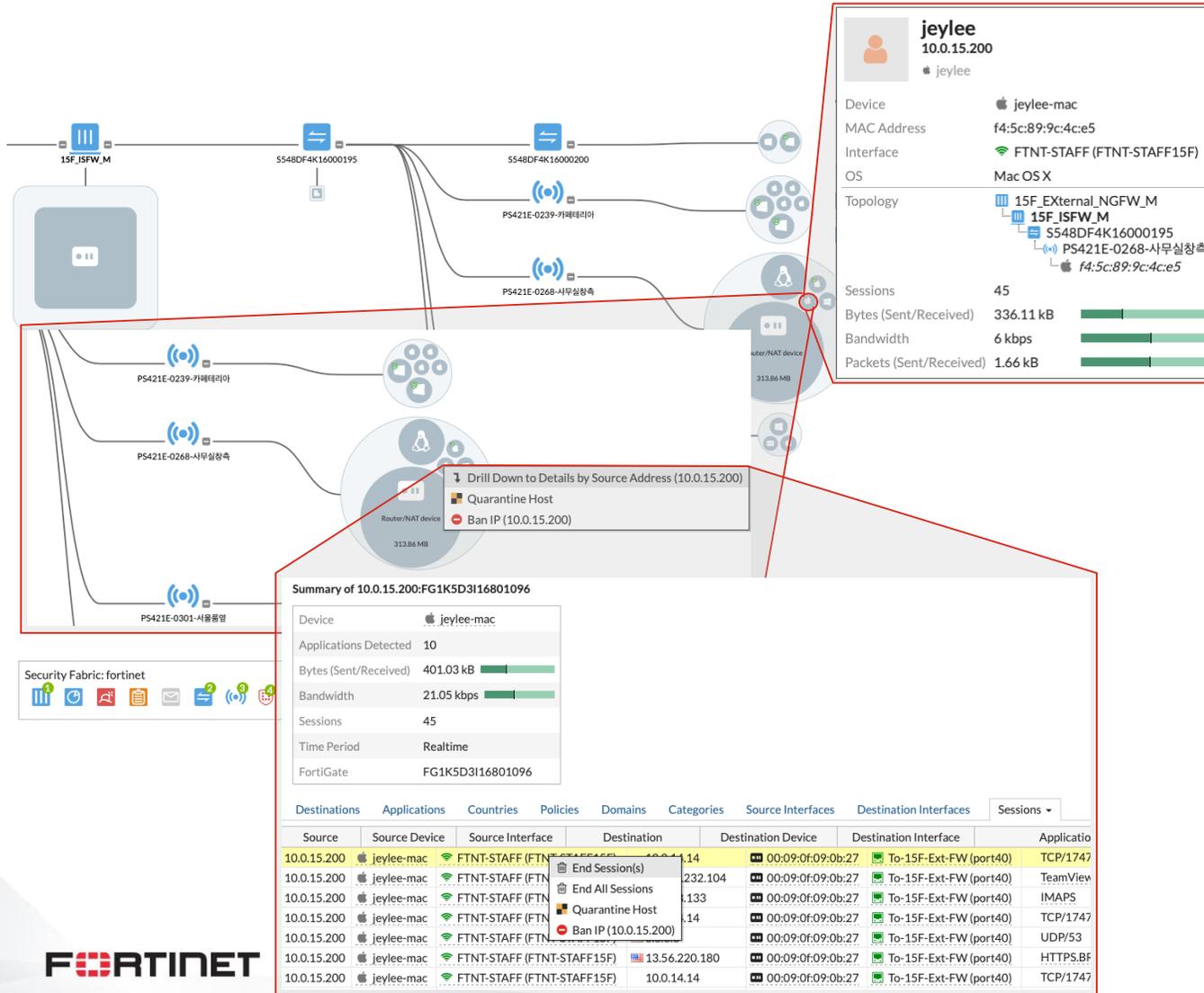
Gartner Peer Insights reviews constitute the subjective opinions of individual end users based on their own experiences, and do not represent the views of Gartner or its affiliates.

Fortinet FortiAP and FortiSwitch Wired and Wireless Networking



네트워크에 보안을 통합한 SD-Branch

네트워크 가시성과 디바이스 가시성



- 유무선 사용자 및 단말기에 대한 실시간 통합 모니터링
- 드릴 다운 형식으로 사용자 상세 모니터링 가능
- 사용자가 사용중인 단말기 정보, 트래픽 이용 현황 등 모니터링

네트워크에 보안을 통합한 SD-Branch

가시성을 기반으로 한 보안

- 전체 네트워크 파악을 위한 탁월한 토폴로지 및 연결된 장비들에 대한 시성
 - 단일 관리 창
 - 본사/데이터센터 및 지사들
 - 모든 장비들(네트워크 장비, 사용자 단말기 등)
- 장비들의 상세 정보와 연결(SSIDs, 포트, MAC 주소, OS 등)
- 확장된 검색 기능
- 침해지표(Indication of Compromise)를 한눈에

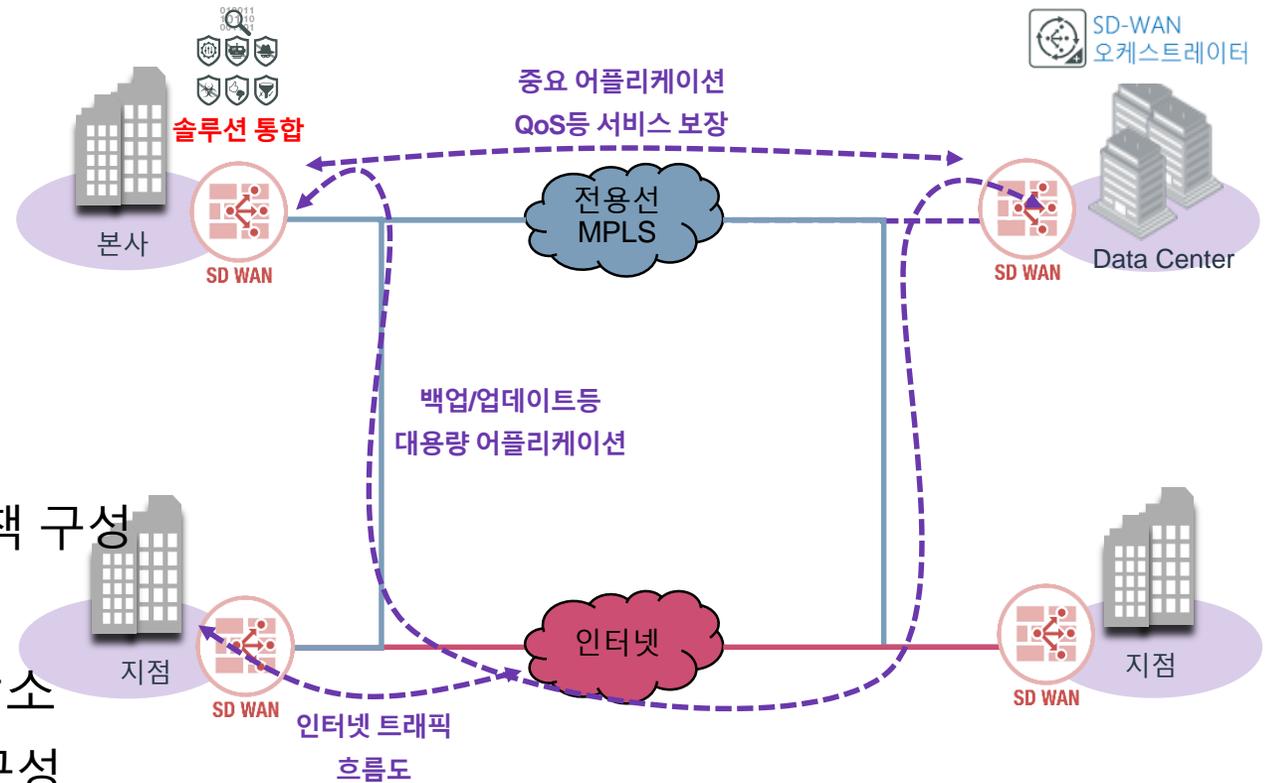
Searchable Information	
Host	Status, Host Name, Server, MAC Address, Other MAC Addresses, IP Address, Interface, Online Interfaces, Device Type, Hardware Vendor / Family, Operating System, Authorized User, Unauthorized User
FortiGate	Serial Number, Host Name, Management IP, Model Label, Operating Mode, Parent, Version, IP Address, AWS Instance ID
FortiSwitch	Serial Number, Name, Version
FortiAP	Serial Number, Name, Version

The image displays a network management interface with two main views. The top view shows a network topology with various devices like FortiGate, FortiSwitch, and FortiAP connected to an Internet cloud. A red diagonal line highlights a specific path. The bottom view is a detailed profile for a device with IP 192.168.77.8, marked as 'Critical Risk' and 'Compromised'. It lists device details like 'Raul P20pro@88:11:96:cc:f8:65', MAC address, IP address, and online interfaces. It also shows hardware (Huawei), OS (Android / 9), and topology information. Performance metrics like sessions (11), bytes sent/received (333.61 kB), bandwidth (7.04 kbps), and packets sent/received (1.44 kB) are shown with progress bars. At the bottom, there are checkboxes for 'Firewall Device Address', 'Firewall IP Address', and 'Quarantine Host'.

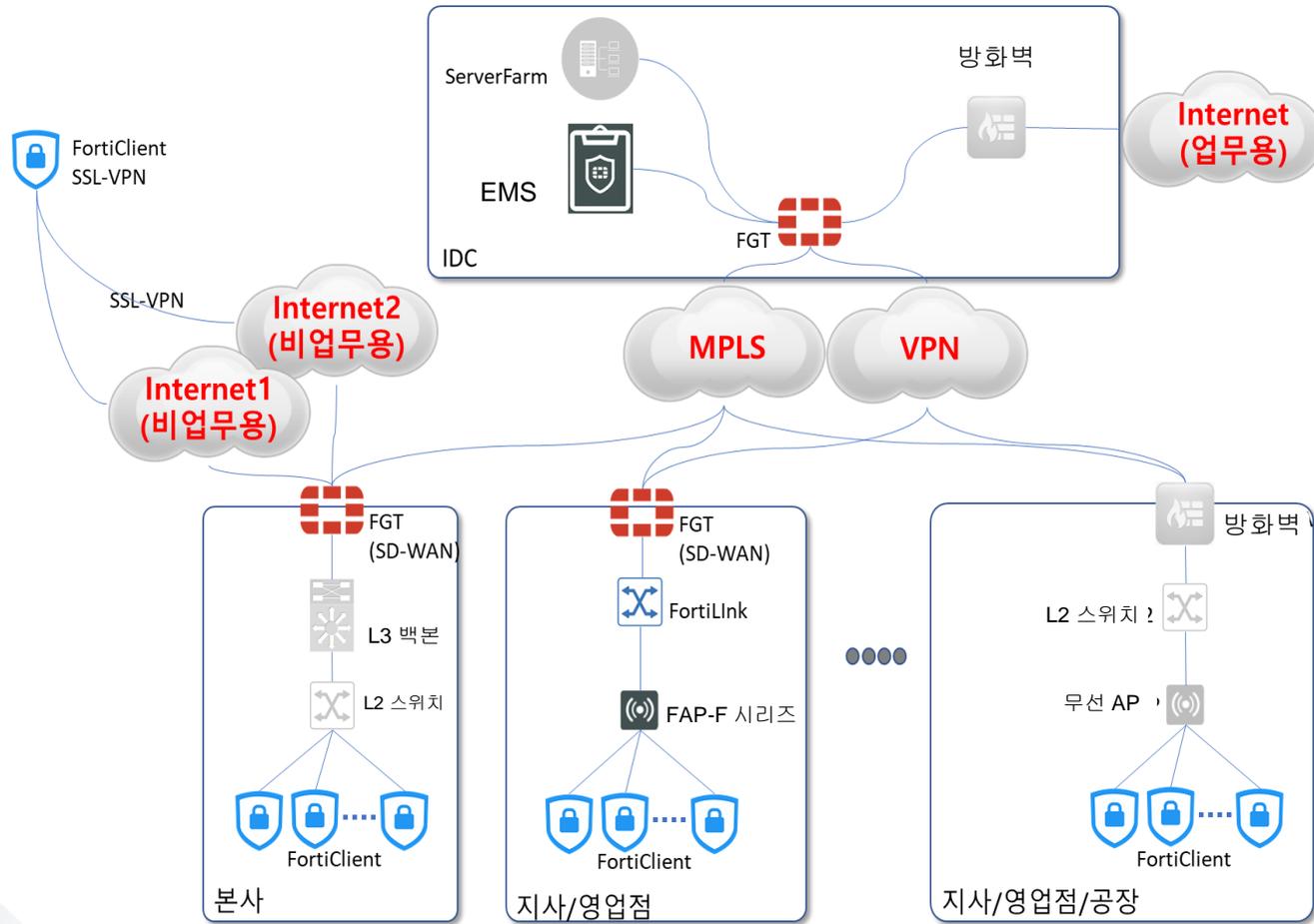
구축사례

구축 사례

- 통합 솔루션 사용으로 중앙 집중 관리
 - 해외 지사까지 통합
- Direct Internet Access로 사용자 만족도 개선
- 대용량 트래픽을 제어하여 업무 대역폭 보장
 - 소프트웨어 UPDATE를 위한 별도 SD-WAN 정책 구성
- 회선을 효율 적으로 사용 -> MPLS 사용량 감소
 - 다수의 회선(Internet/MPLS)에 대해 SD-WAN 구성
 - 인터넷 전화 등 어플리케이션 인지에 대해 품질 우선 순위 적용

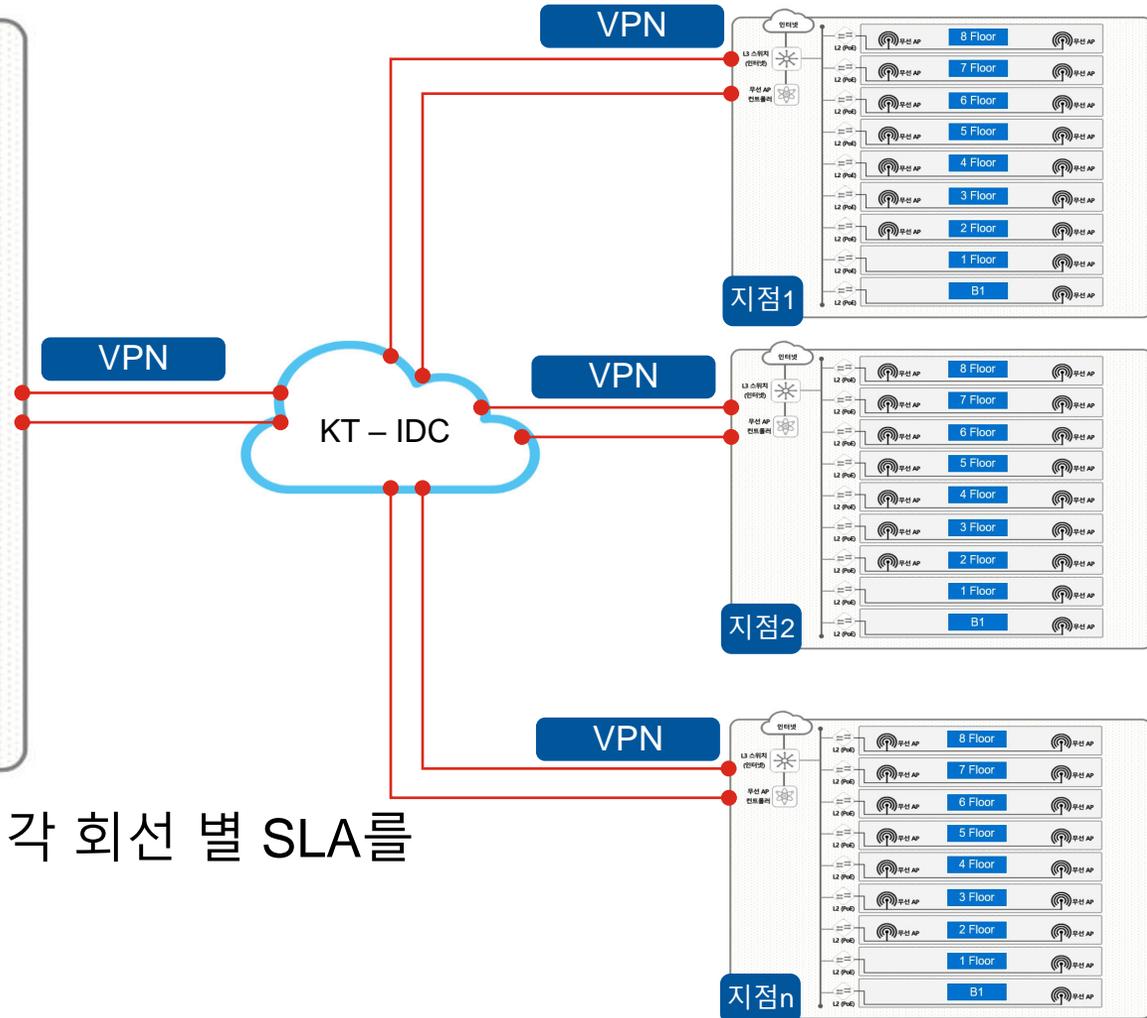
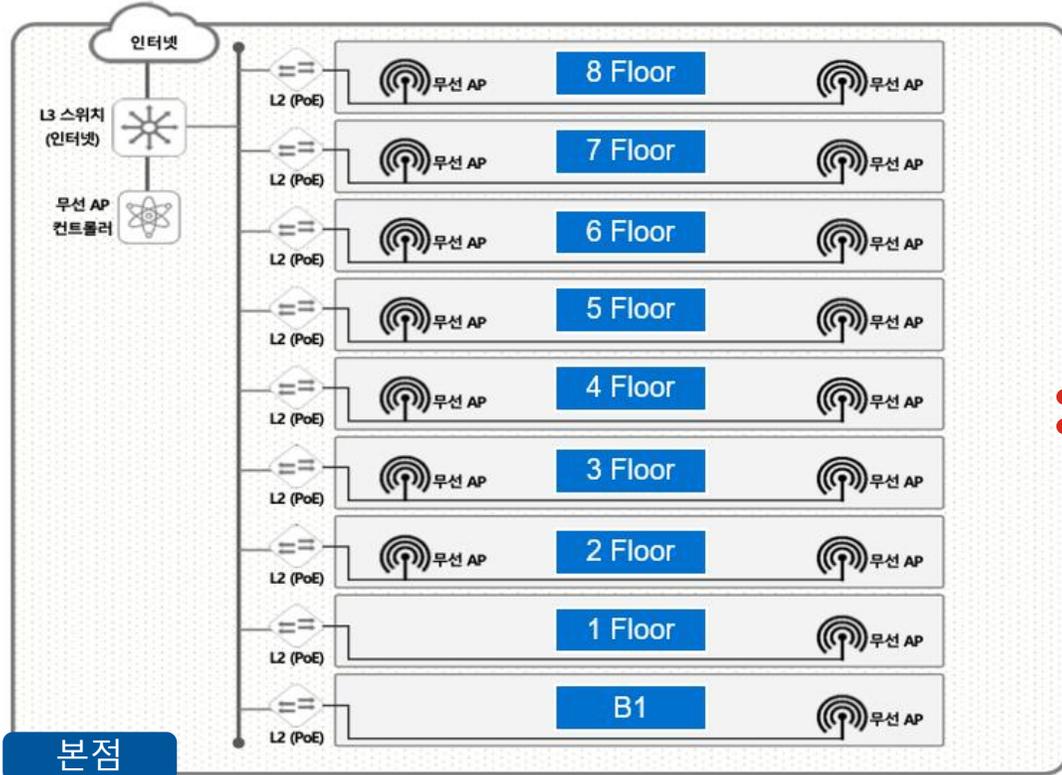


구축 사례



- 본사와 지사간 서비스 가용성 증대 효과
- 엔드포인트 단말기의 AV백신, 컴플라이언스 준수 유무 체크
- 지사 내부 SD-Branch 구축으로, 유무선 서비스 및 접속 보안 효과
- 하나의 화면에서 전체 네트워크 모니터링

구축 사례



- IDC 센터와 본점 및 각 지사 간 VPN 구성 : 각 회선 별 SLA를 체크하여 회선의 품질 모니터링
- 회선의 효율성으로 대역폭 향상

맺음말

포티넷 시큐어 SD-Branch를 통해 얻을 수 있는 주요 장점

• 네트워크에 보안이 통합된

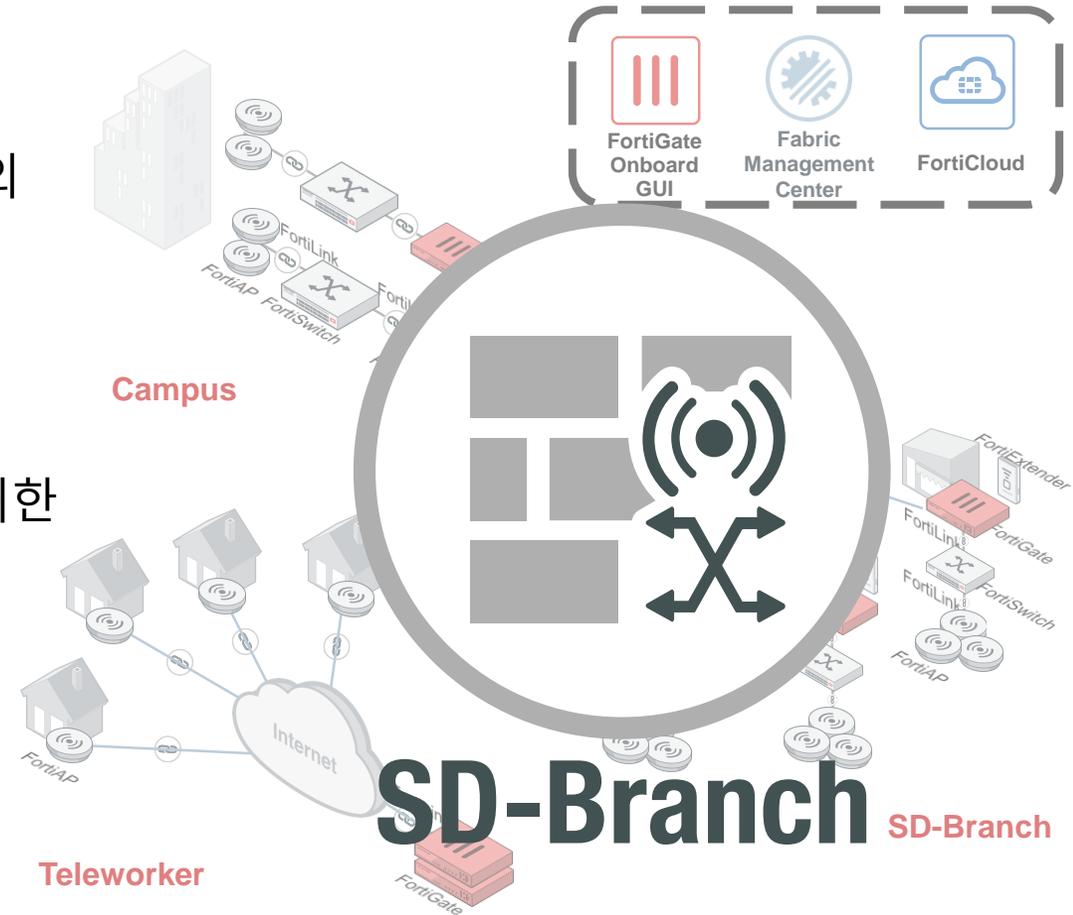
- 더 엄격한 보안 통합을 공급하는 업체는 없음
- 포티스위치와 포티AP는 포티링크를 통해 차세대 방화벽의 확장으로 통합
- OT/IoT를 위한 NAC 기기 검색, 가시성 보안 및 이상 탐지

• 복잡성 제거

- 보안, 네트워크 액세스 및 SD-WAN을 관리 및 운영하기 위한 단일 관리 창
- 문제 해결의 단순화
- 구축 및 확장의 민첩성 향상
- 이해하고 구현하기 쉬운 라이선스

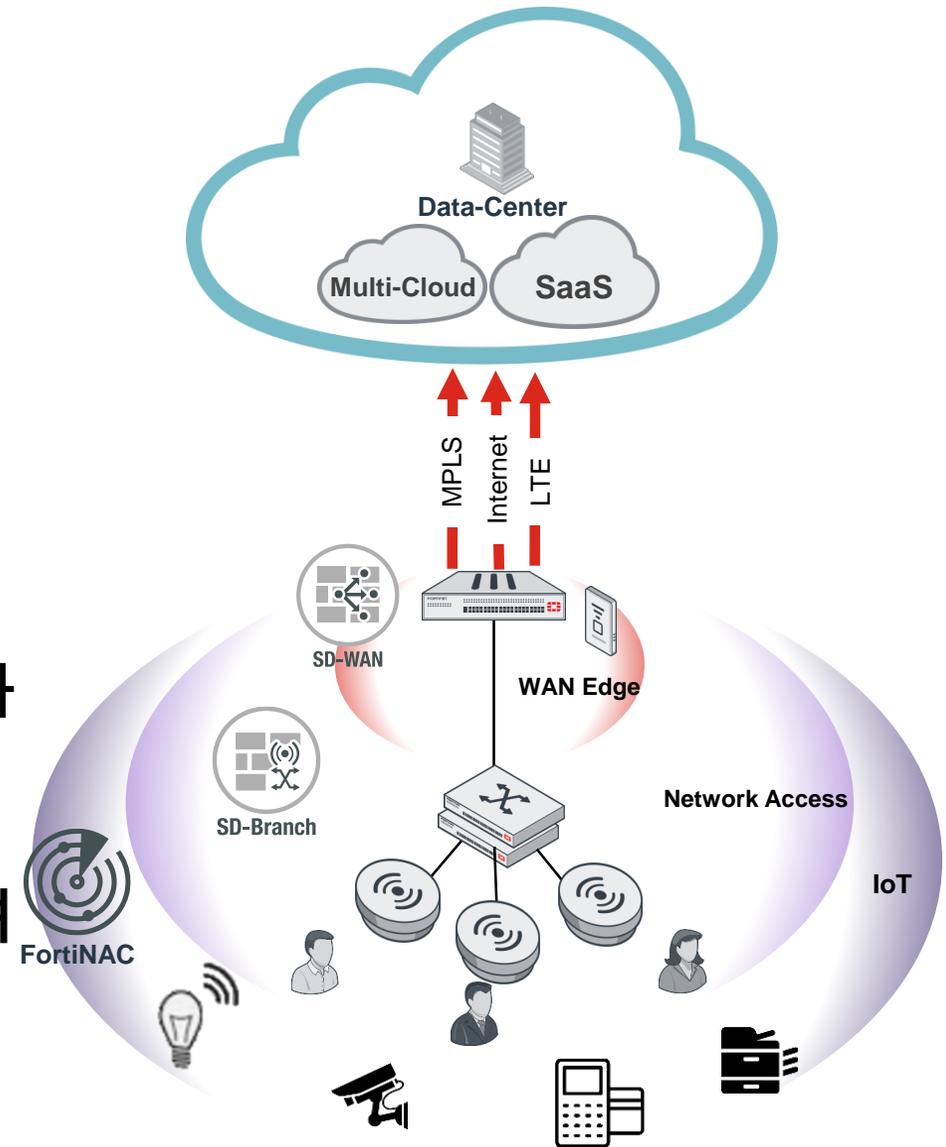
• 비용 효과적인 아키텍처

- 기능 구현을 위한 복잡한 라이선스 없음
- AP 및 스위치 연동, SD-WAN 기술 구현을 위한 라이선스 없음



요약

- 디지털 혁신은 네트워크 액세스의 급변화를 발생시킴
- 클라우드 등 SD-WAN을 통해 다양한 액세스 환경을 제공함에 따라 더 많은 네트워크 에지가 생성되고 이에 따라 네트워크 보안이 주요 관심사
- 포티넷 시큐어 SD-Branch는 네트워크 엣지에 대해 다양한 가시성 기반으로, 우수한 애플리케이션 경험과 업계 최고의 보안을 동시에 제공
- 이로 인해 비즈니스 업무 환경을 단순화하고 보호하며 네트워크 및 디바이스 엣지의 관리 및 가시성을 가능하게 함



F **ORTINET**®