시큐리티 패브릭을 통한 네트워크 통합 보안

- 가시성을 기반으로 쉽고 빠르고 편하게 네트워크를 관리/제어

포티넷시큐리티 코리아 이창운 이사

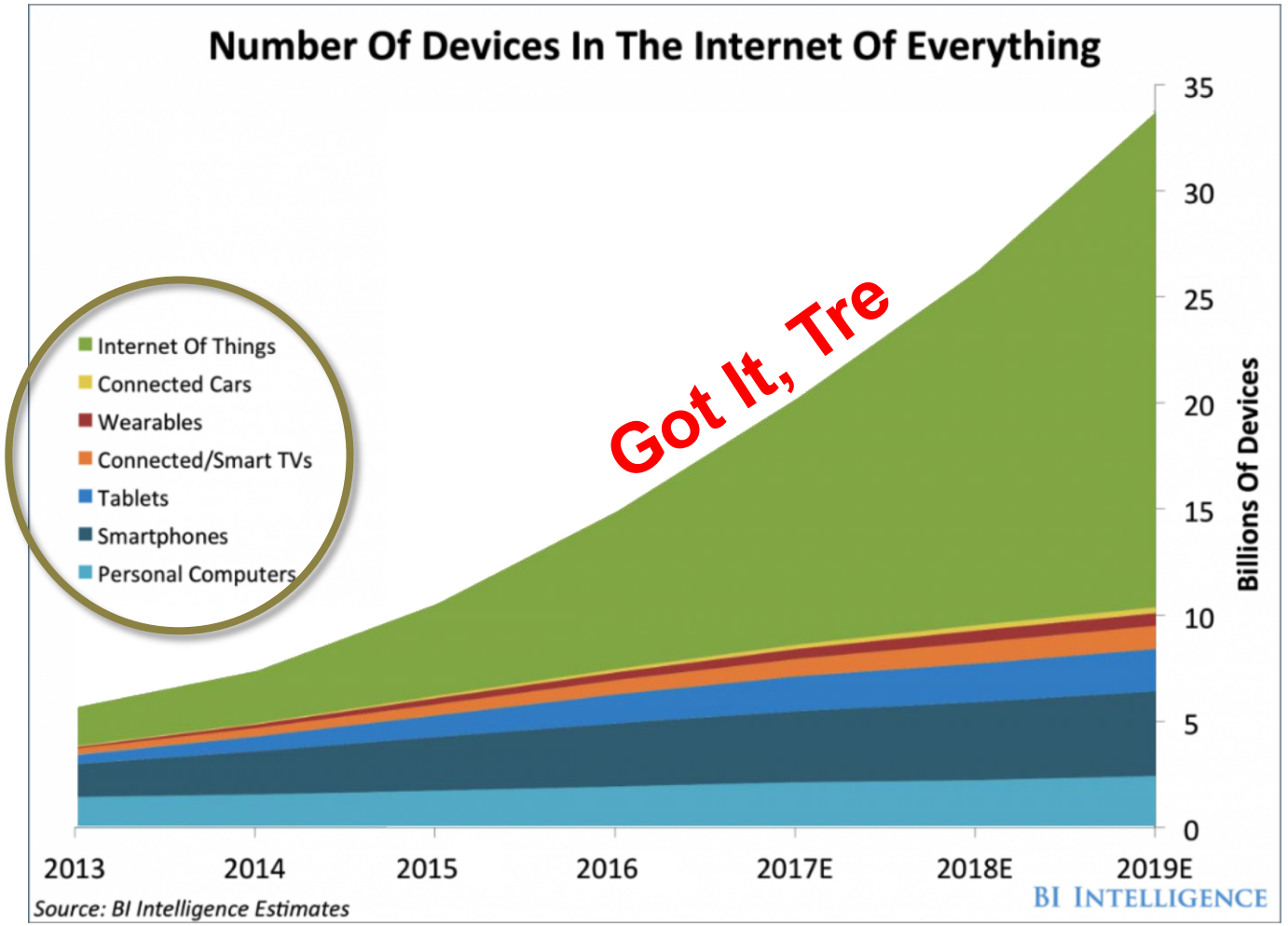
2018년 4월 26일

시장동향 : 디바이스의 성장은 지칠 줄 모르고 계속...

IoT 및 스마트 기기에 의한 성장 주도

- 약 330억 개의 장치가 2020년까지 연결될 것으로 예상 *
- 네트워크에 접속되는 많은 새로운 장치 유형
- 2020 년에는 엔터프라이즈 공격의 25%가 IoT 기기를 통해 *

* Source: Gartner



가트너 업계 견해

유선 및 무선랜 엑세스 매직쿼드런트.

- 기업들은 가트너에게 유무선 액세스 네트워크 전반에 걸쳐 **공통된 보안 정책 집행 및 관리**를 선호한다고 계속 말하고 있습니다. 최근 가트너의 기업 고객 설문 조사에서 **70 % 이상의 고객이 '단일 벤더의 액세스 레이어 솔루션 배포를 선호한다'**라고 응답했습니다.
- 또한 대기업 캠퍼스 환경 외에도 기업의 원격 지사 사무실 등 다양한 구현 시나리오를 위해 사설 클라우드 또는 공용 클라우드에 사내 구축 형 네트워크 응용 프로그램을 배포 할 수 있는 유연성이 필요하다고 들었습니다.

가트너에서 바라본 유무선 액세스 통합 보안

- 포티넷의 **핵심인 차세대 UTM 방화벽 및 기타 보안 기능 등을 중심으로 통합 액세스 네트워크에 통합한 시큐어 액세스 아키텍쳐(Secure Access Architecture)**는 기업의 보안 침해 및 데이터 탈취가 널리 알려지면서 네트워크 지향적인 위협에 대한 인식을 높이는 동시에 가치를 제공합니다.


Gartner

This research note is restricted to the personal use of pnewton@fortinet.com.

G00291908

Magic Quadrant for the Wired and Wireless LAN Access Infrastructure

Published: 30 August 2016

Analyst(s): Tim Zimmerman, Christian Canales, Bill Menezes, Danilo Ciscato

...enterprise ... wired and wireless access ... vendors based on their ability to offer the same network applications across both the wired and wireless infrastructure and address new IoT challenges.

Strategic Planning Assumption

By 2020, ... will spend 10 times more on network service applications than the associated access point and switch hardware components, up from less than 2% reported today.

Market Definition/Description

This document was revised on 2 September 2016. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

This market consists of vendors that supply wired and wireless networking hardware and software that provides device connectivity to the enterprise infrastructure access layer. These devices can be laptops, tablets, smartphones, sensors and any device that is fixed or mobile which is ... to a ... port ... to an access point at the edge of the enterprise ... These ... networking components may include:

- Hardware — Wireless access points, wired switches, controllers
- ... applications, including:
  - Network management
  - Guest access
  - Onboarding services
  - AAA security/authentication
  - Policy enforcement

This research note is restricted to the personal use of pnewton@fortinet.com.

IT가 직면한 도전 과제들

- 증가하는 단말기 수, 장치 유형, 응용 프로그램 및 사용 사례
- 증가하는 사이버 위협, 외부 및 내부
- LAN / WLAN 및 보안을 위한 개별 정책은 더 이상 수용 할 수 없는 사안.
- 통합 관리 서비스 필수
  - » 가시성
  - » LAN 및 WLAN 관리
  - » 위협 관리
  - » 단일 리소스에서 제어 및 관리

우리 회사의 보안 태세에 100 % 확신하고 싶습니다.

액세스 레이어 시장 상황

고객이 스위칭 및 무선 인프라에 변화를 주려고 하는 이유가 무엇일까?

보안 범위 개선

- 64,199 건의 사건들, 2,260 건의 위반(Verizon DIBR 2016)
- 액세스 레이어는 가장 광범위한 위협 요소

트래픽 증가

- 가트너에 의하면 2017 년에 84 억개의 "***Things***" 이 네트워크에 연결되었고, 2016 년 보다 31 %가 증가.
- 빠른 프로토콜 및 데이터 집약적 인 애플리케이션

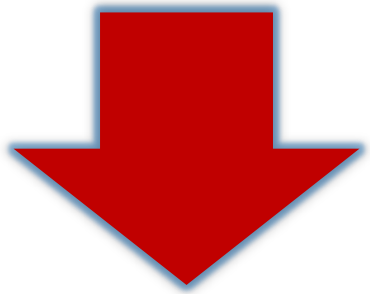
관리의 단순화

- 사용자들은 유선, 무선 및 VPN 등에 일관된 경험을 기대.
- 관리자는 보안의 일관성 기대

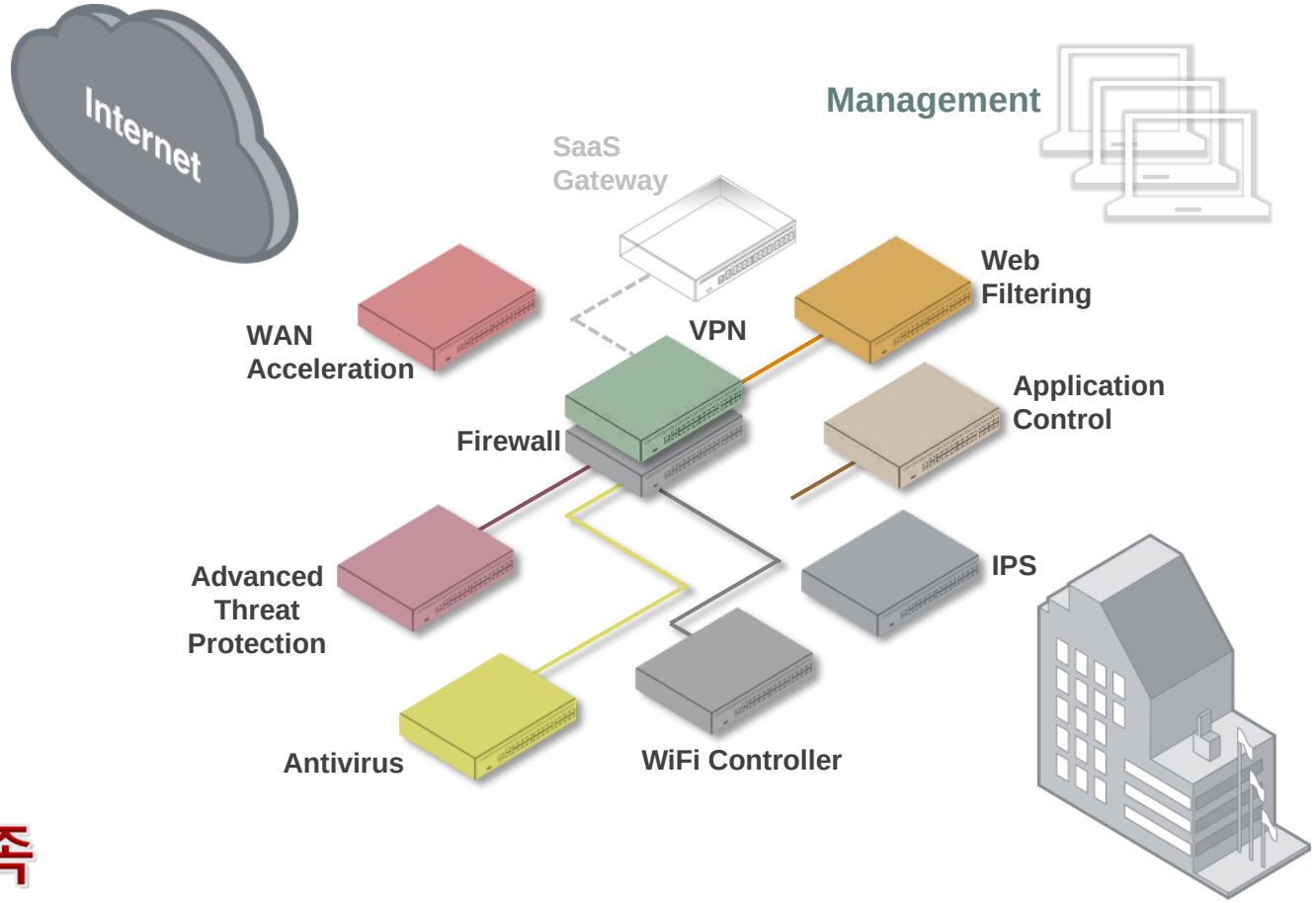
전형적인 통합 보안 액세스 접근법 : 복잡성

복잡성은 경계대상이자 敵(적)!!!

- 많은 포인트 솔루션/플랫폼
- 많은 관리 콘솔들
- 중복 투자 등 비용 증가
- 일관성 없는 정책 및 네트워킹
- 다양한 업그레이드 주기



- **느리고 허술한 보안 대응**
- **유지보수에 대한 자원의 한정/부족**
- **네트워크 구성을 복잡하게 만듦**



기존 보안 운영의 어려움

높은 보안 요구 사항

- 높은 규정 준수 요구
- 해킹의 타겟이 되어 높은 수준의 방어 전략 필요

관리 부하

- 업무량에 비해 관리 인력 부족
- 서비스 관리에 집중, 내부 관리 리소스 투입 불가능

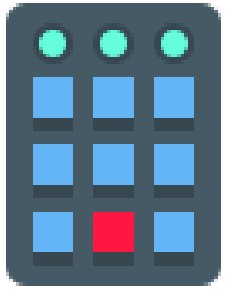
유연성 요구

- 대기업 및 금융기관과 같은 통제 불가능

네트워크 보안의 두가지 영역

보안성을 높이면서 동시에 보안강화로 인한 불편함을 줄일 수 있습니다

통제 영역



“필요한 것만 허용 ”

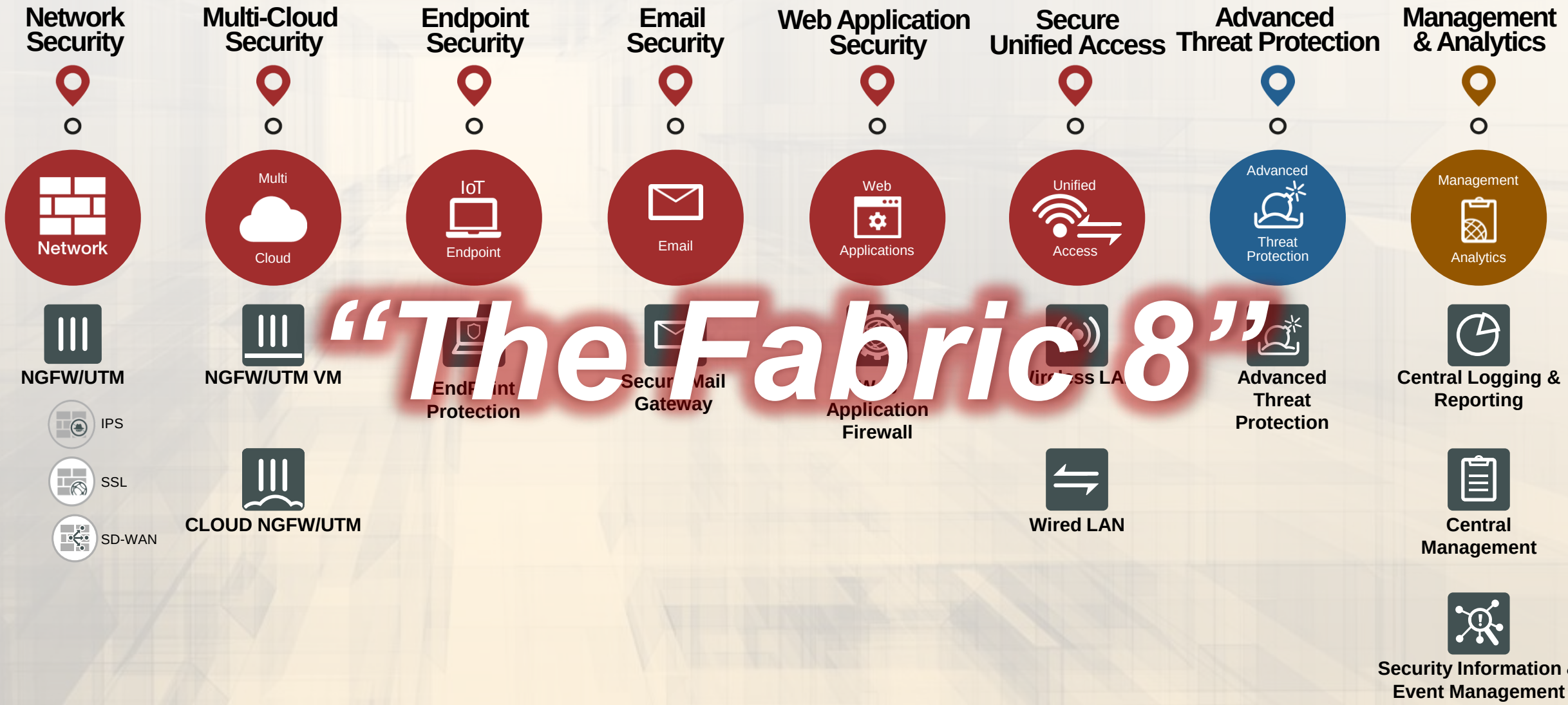
- 방화벽 (Firewall)
- 어플리케이션 컨트롤 (Application Control)
- 웹필터 (WebFilter)
- 웹방화벽 (Web Application Firewall)

공격 방어 영역

“공격인 것만 방어”

- IPS (Intrusion Prevention System)
- AV (AntiVirus)
- APT (Sandbox)

SOLUTIONS ARE DEAD, LONG LIVE SOLUTIONS



"The Fabric 8"

NOT A K-POP GROUP

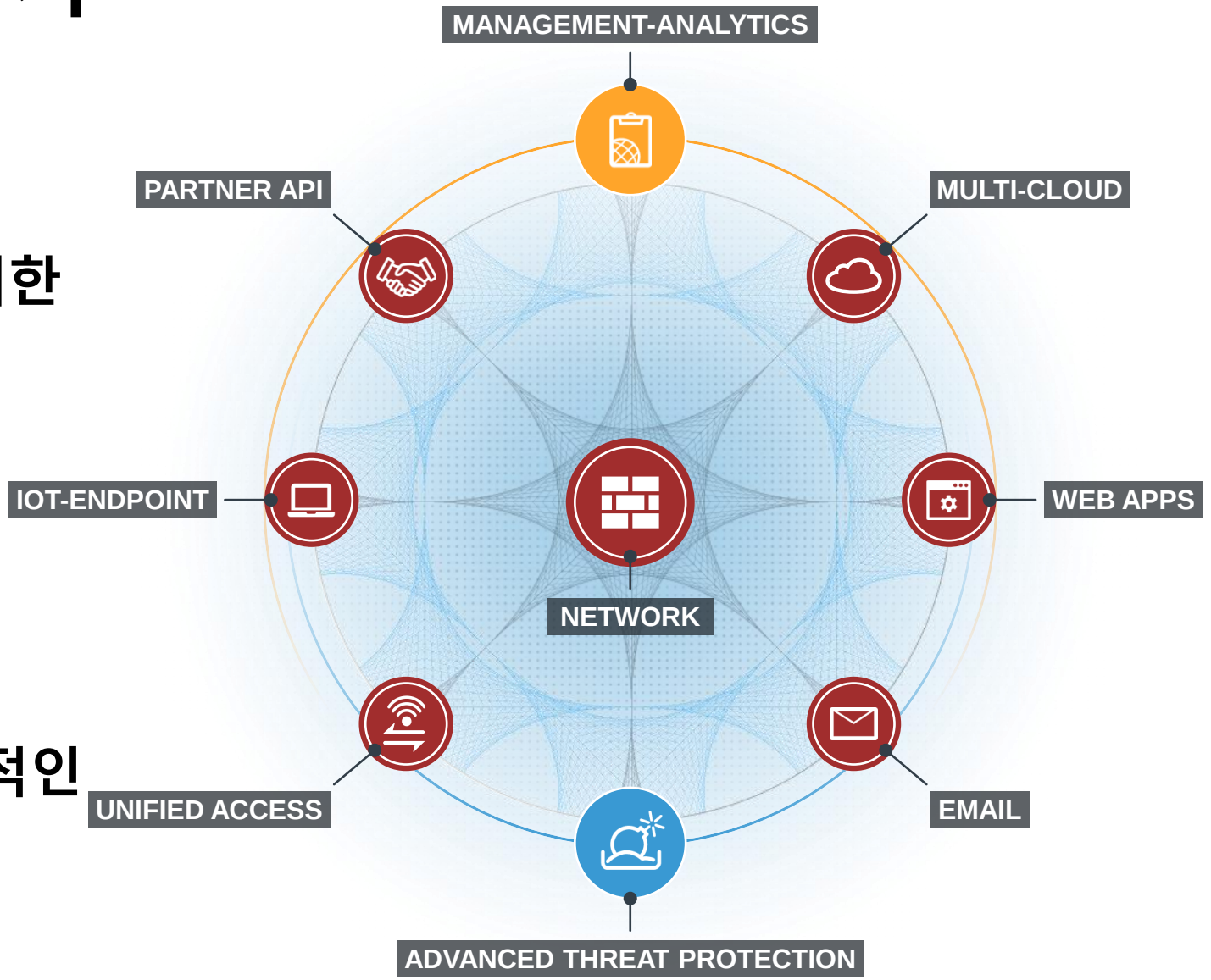
시큐리티 패브릭 아키텍쳐

보안 아키텍쳐가 다음을 제공:

BROAD 디지털 공격 영역에 대한 가시성 및 보호

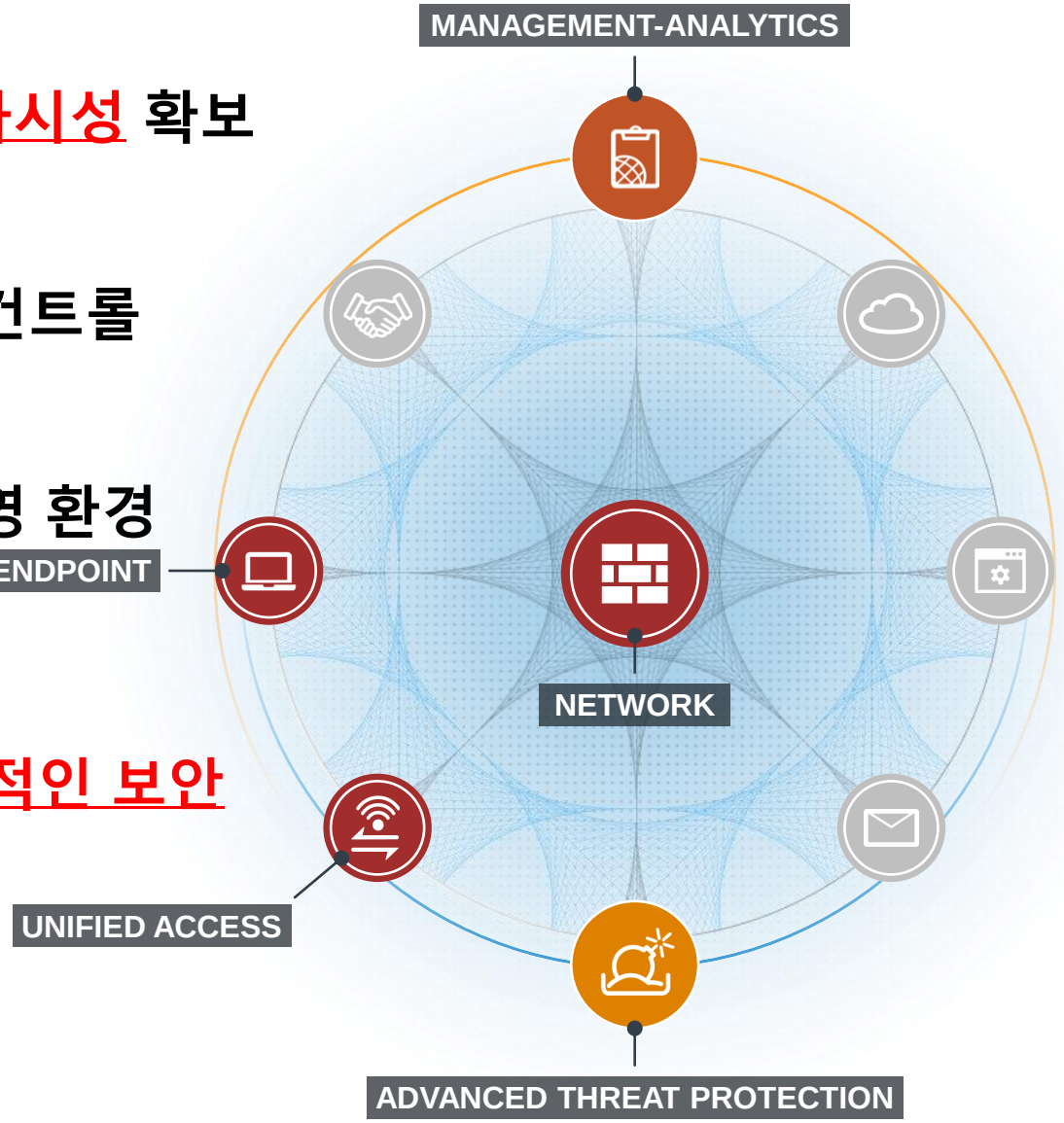
INTEGRATED 지능형 공격 위협 탐지

AUTOMATED 대응 및 지속적인 신뢰 평가



시큐리티 패브릭 기반 통합 보안 액세스의 이점

- 유무선 네트워크, 인프라 전반에 대한 보안 가시성 확보
- 단일 창을 통한 전체 네트워크 정보 습득 및 컨트롤
- 운영 단순화, 전문 지식 없이 높은 수준의 운영 환경 제공
- 인프라에서 적용되고 시행되는 공용 및 일관적인 보안 정책
- 배포의 용이, 고 가용성 및 관리의 단순화



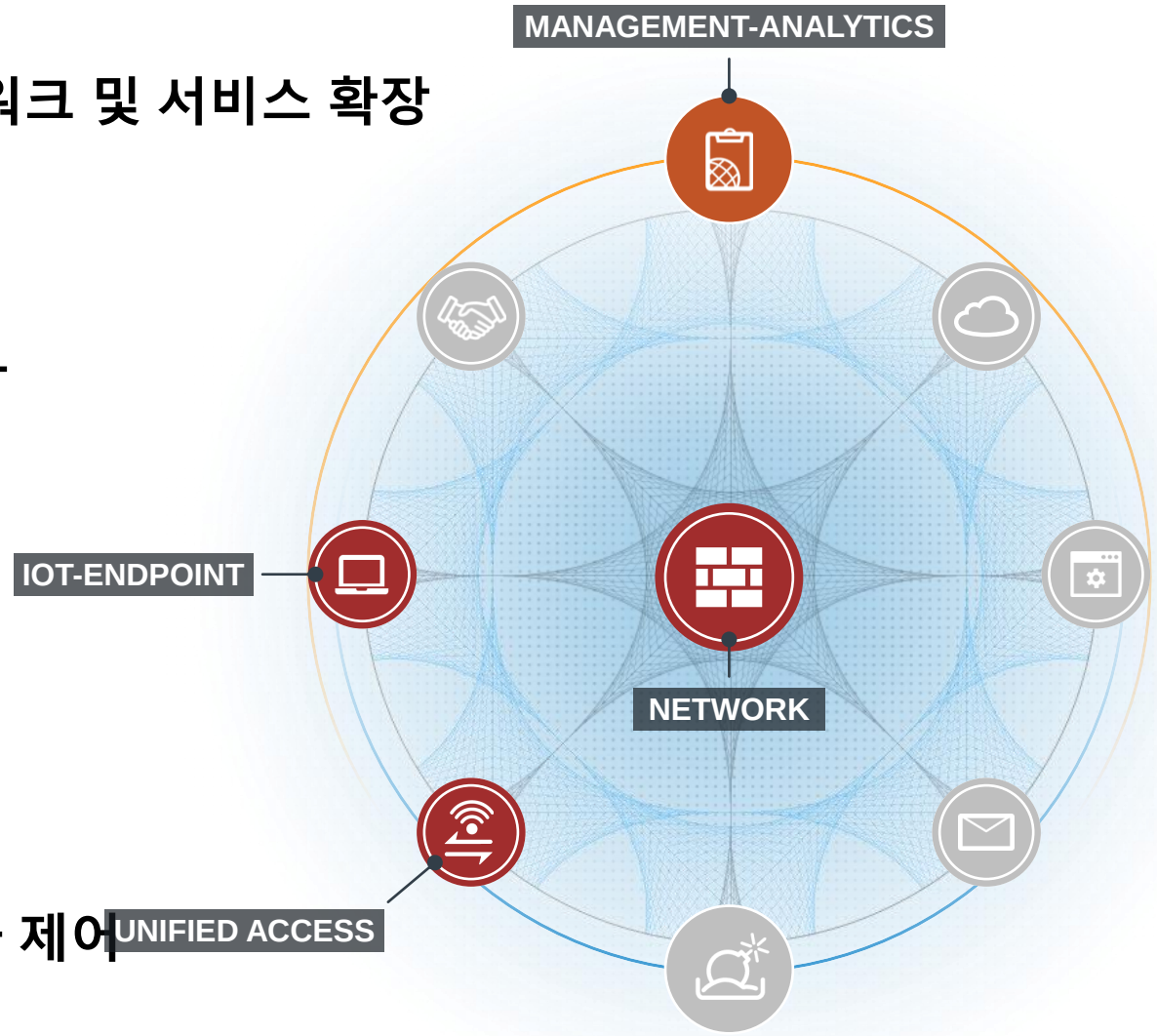
유무선 보안 통합 솔루션이 가져올 장점

보안 서비스 세트 완성
차세대 UTM 방화벽를 중심으로 네트워크 및 서비스 확장

스위치 구성 및 제어
포티링크 프로토콜을 통해 스위치 통합

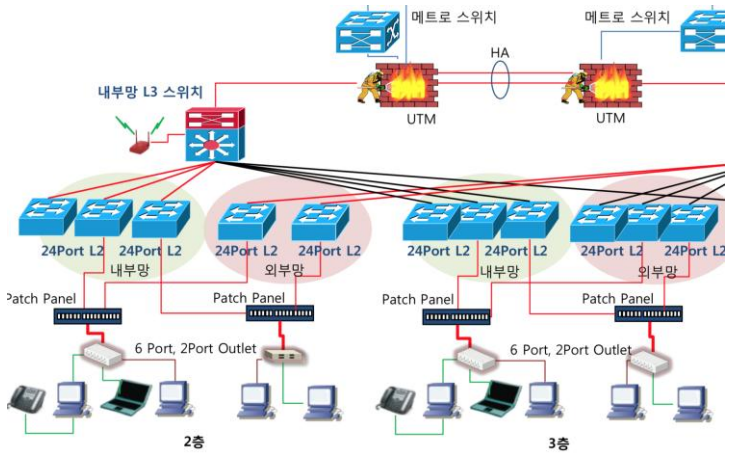
AP 구성 및 제어
최고의 성능과 간편한 구축

단일창을 통한 관리
무선, 유선 및 보안 통합 관리와 사용자 제어



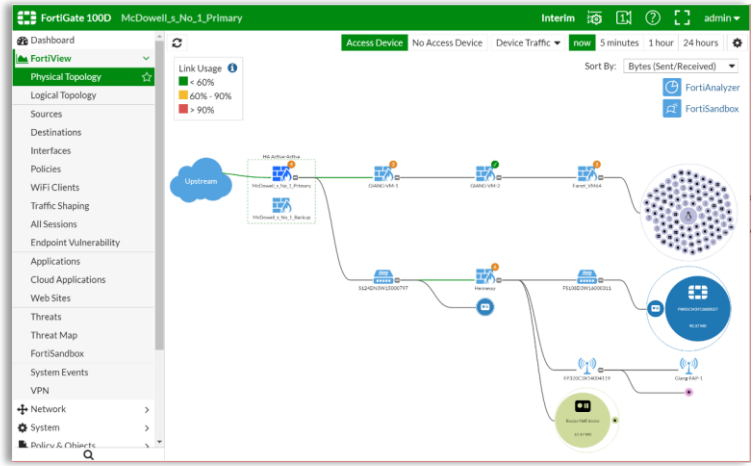
AS-IS TO-BE (인프라 지능화)

AS-IS



- 보안, 네트워크 별도 관리 필요
- 전문적인 네트워크 운영 지식 필요
- 보안 사고 시 대응이 어렵고 많은 시간 필요

TO-BE



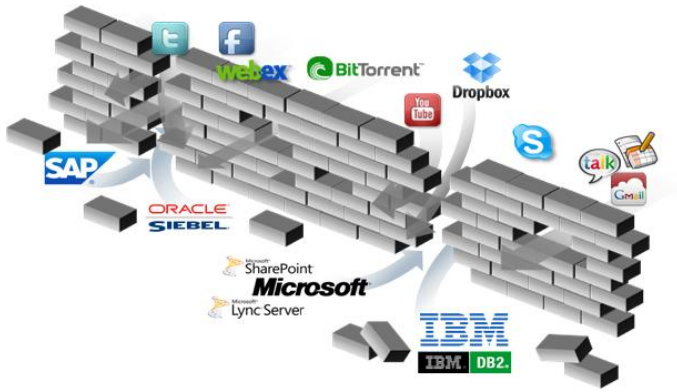
- 네트워크, 보안 통합 관리
- 손쉬운 보안, 네트워크 관리
- 보안 사고 시 짧은 시간에 손쉽게 대응 가능

장점

- Security Fabric 을 이용하여 네트워크-보안 통합 구성
- 사용자 그룹 별로 정책 수립 가능
- 사고 발생 시 사용자 별로 추적, 로깅 가능
- 추가 보안강화를 위한 2Factor 인증 등 도입 가능
- 단일 화면에서 전체 네트워크-보안 관리

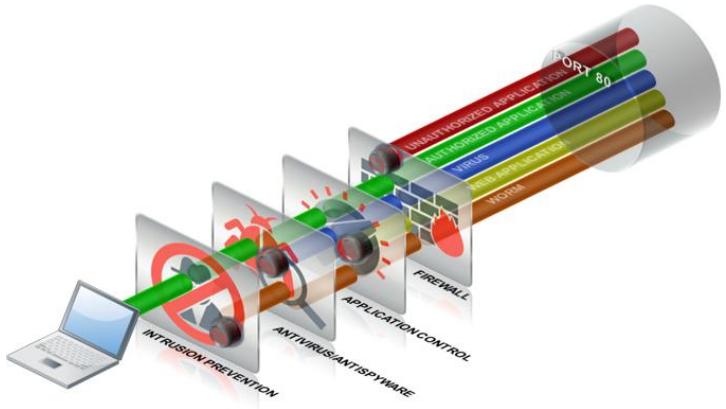
AS-IS TO-BE (보안 강화)

AS-IS



- IP 와 PORT 기반으로 정책 적용
- 다양한 우회 방법 차단 불가능 (PROXY, 원격컨트롤, 터널링 등)
- C&C 서버를 통한 공격 무방비

TO-BE



- 다양한 NGFW 기능 적용으로 높은 가시성 제공
- 방화벽 우회공격기술 차단 (APPCTRL, WEBFILTER, AV, IPS 등)
- 풍부한 C&C 서버 접속 데이터베이스 적용

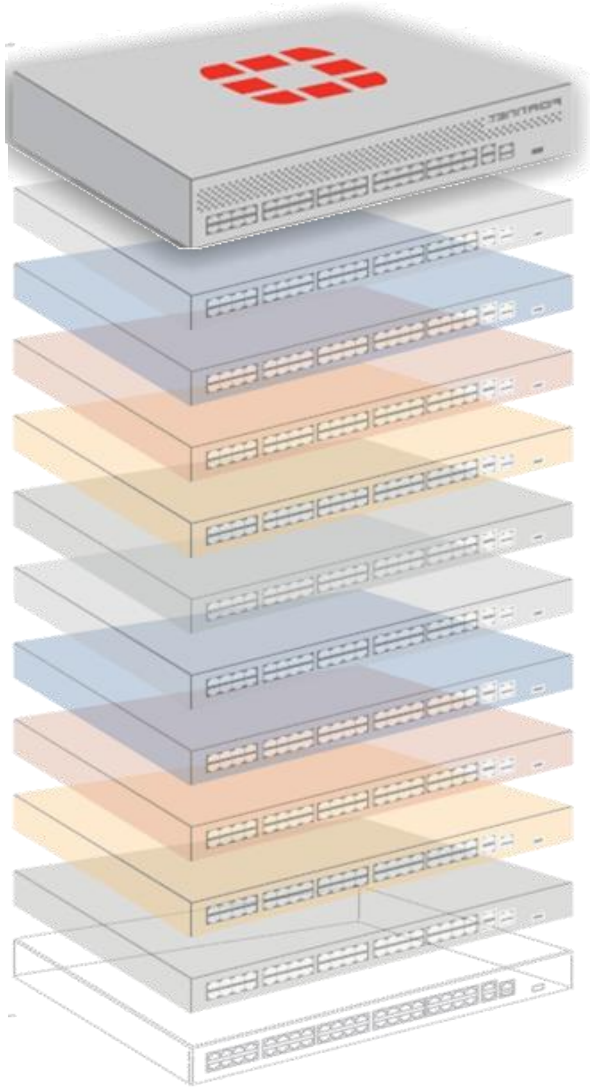
장점

글로벌 인텔리전스 DB 연동을 통한 보안 강화 방안

- Compliance 준수 (TCP 80 외에 다양한 높은 수준의 방어 가능
- 기존의 Legacy 방어는 다양한 공격을 방어할 수 없습니다.
- 보안 강화를 위한 다양한 기능 활성화 (AppCtrl, App, Webfilter, AntiVirus 등)
- Bot, C&C 서버 통신을 방어하기 위한 다양한 DB 제공 (IP, DNS, AppCtrl, WebFilter)

보이지 않는 것을 보이게 만들기

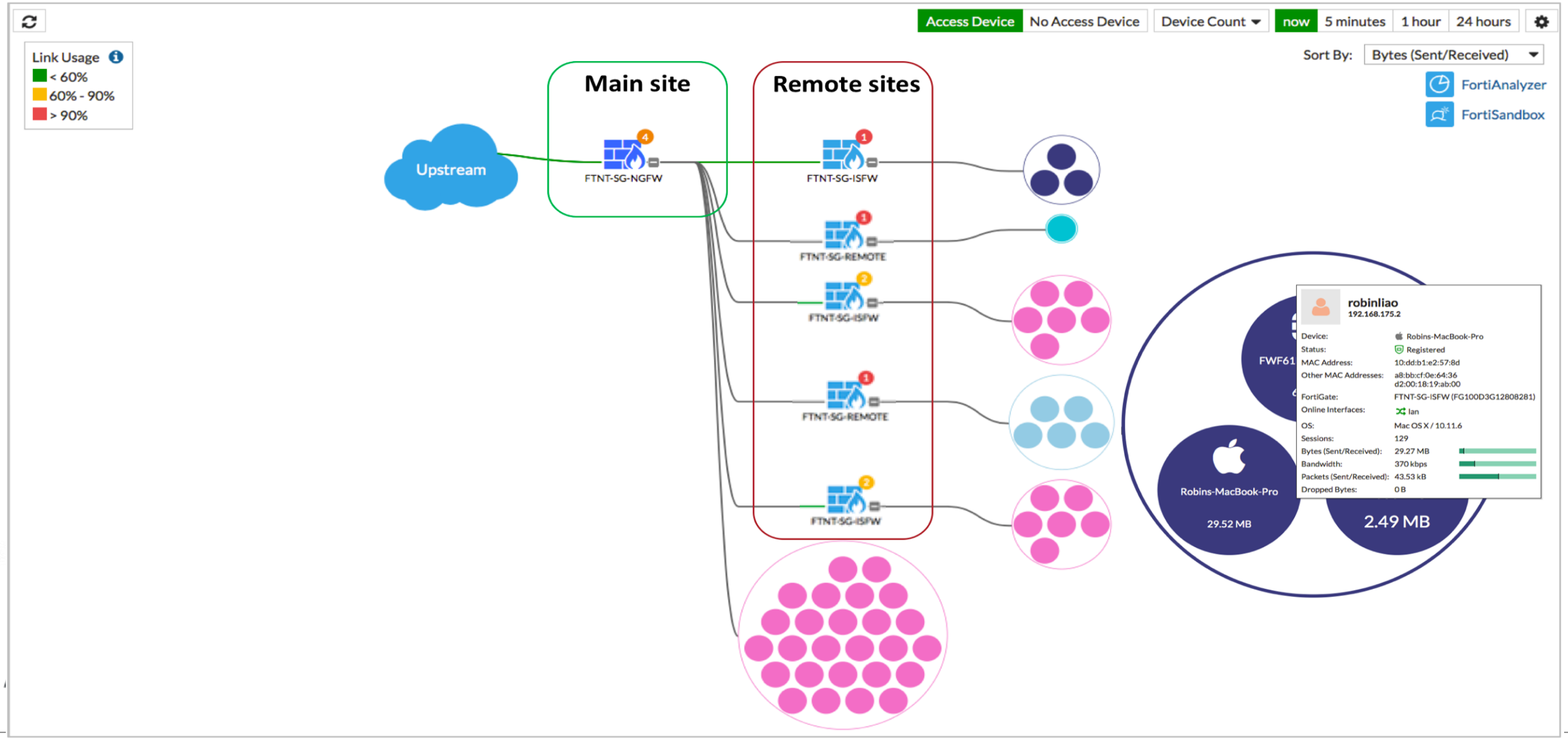
포티넷이 제시하는 유무선 통합 보안 액세스 접근법



차세대 UTM 서비스

- **NEXT GENERATION FIREWALL**
- *Virtual Private Networks (VPN)*
- ***Application Control***
- *Intrusion Prevention Services (IPS)*
- *Web Filtering*
- ***Anti-Malware***
- *Data Leakage Protection*
- ***Advanced Threat Protection***
- *WAN Acceleration*
- **무선랜 컨트롤러**
- **스위치 컨트롤러**

시큐리티 패브릭을 통한 보안 전략



전형적인 네트워 인프라 : 제한적인 가시성

제한된
APP/DATA의 정보

제한된
단말기/사용자들의
상태 및 가시성

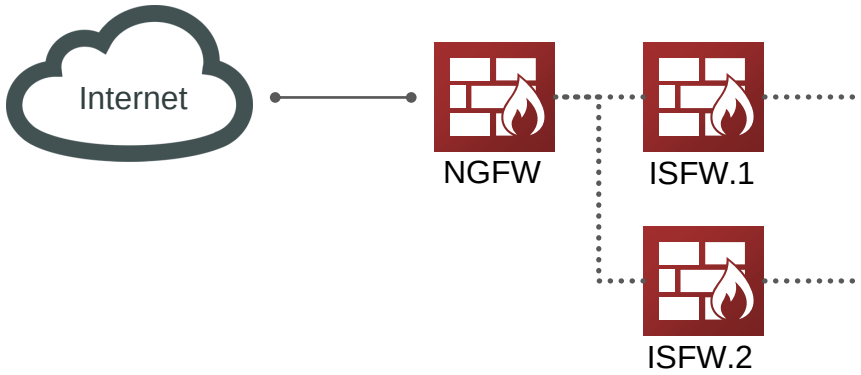
시큐리티 패브릭을 도입한다면...

시큐리티 패브릭을 도입한다면...

패브릭 기능으로 다른 NGFW 및 기기들을 검색

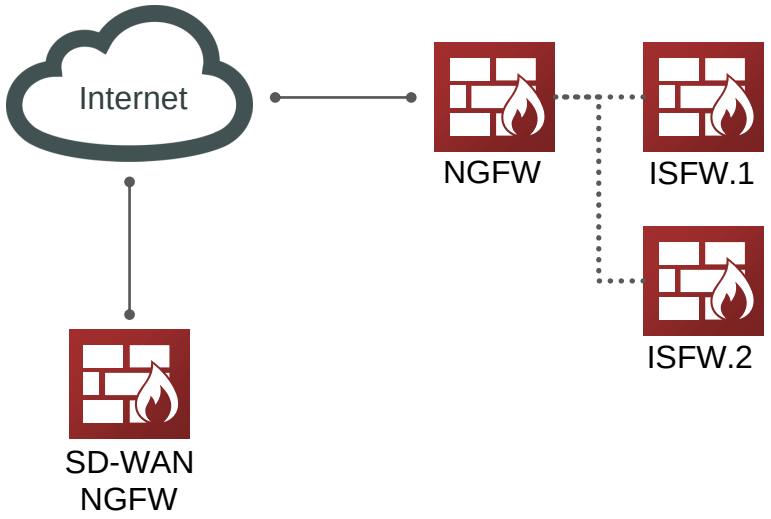
Fabric Integration

내부 다른 방화벽들이 보이고 보호



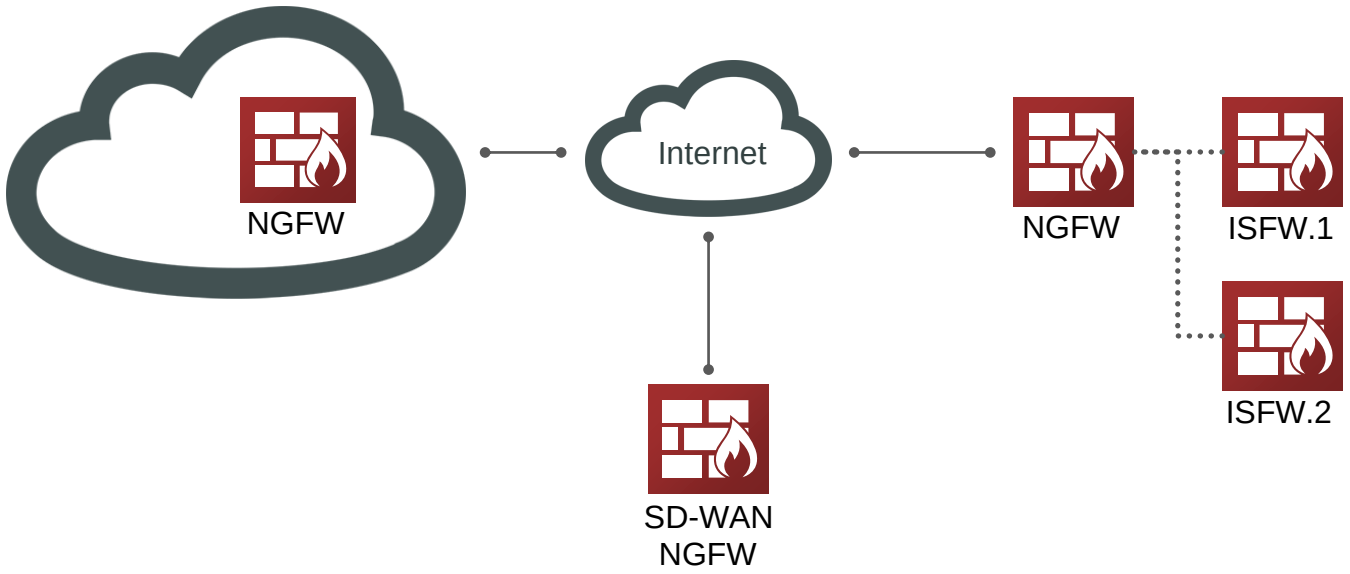
3

SD-WAN 방화벽이 보이고 보호

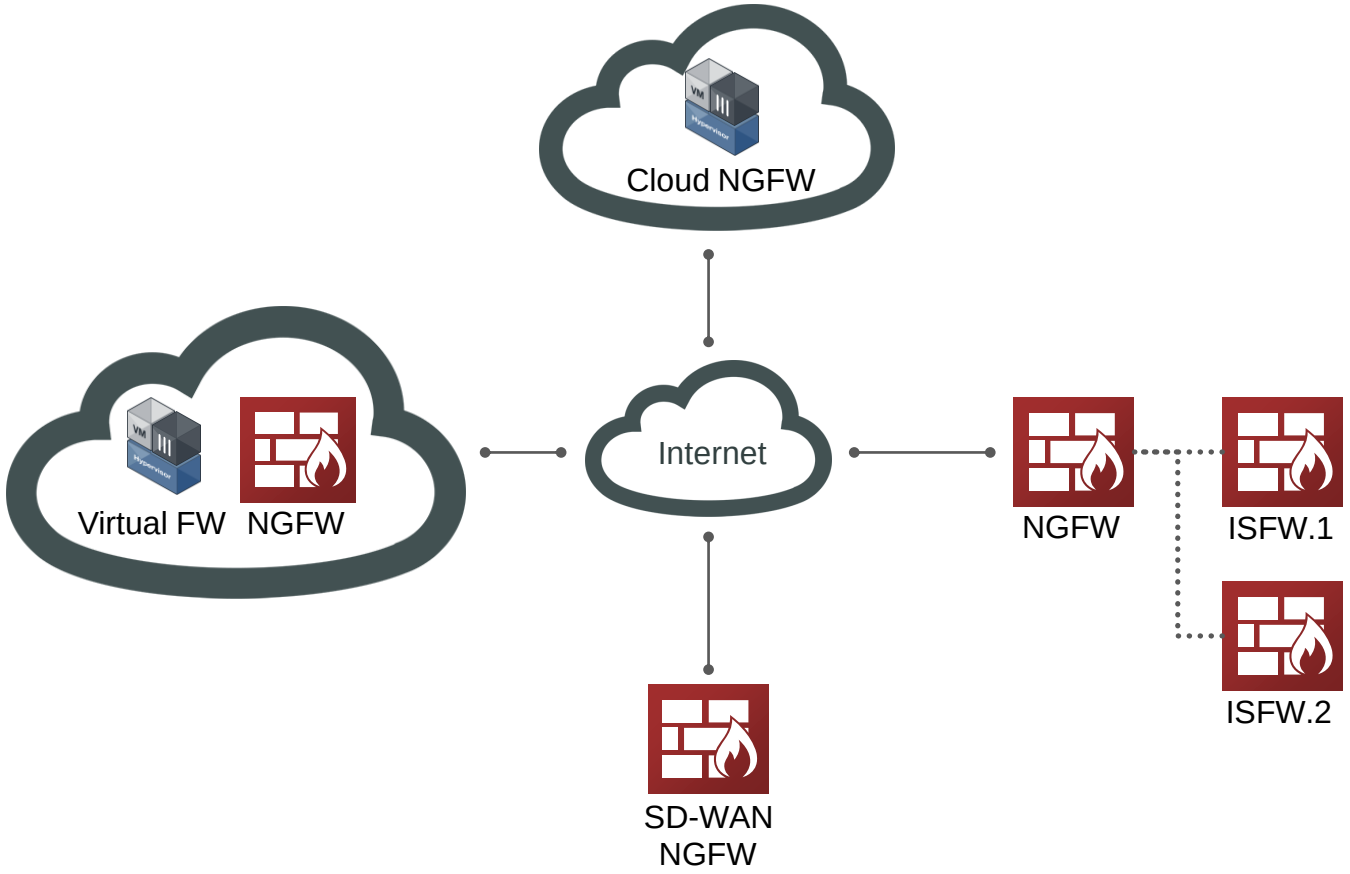


4

DC 방화벽이 보이고 보호



VM 및 클라우드 기반 방화벽이 보이고 보호

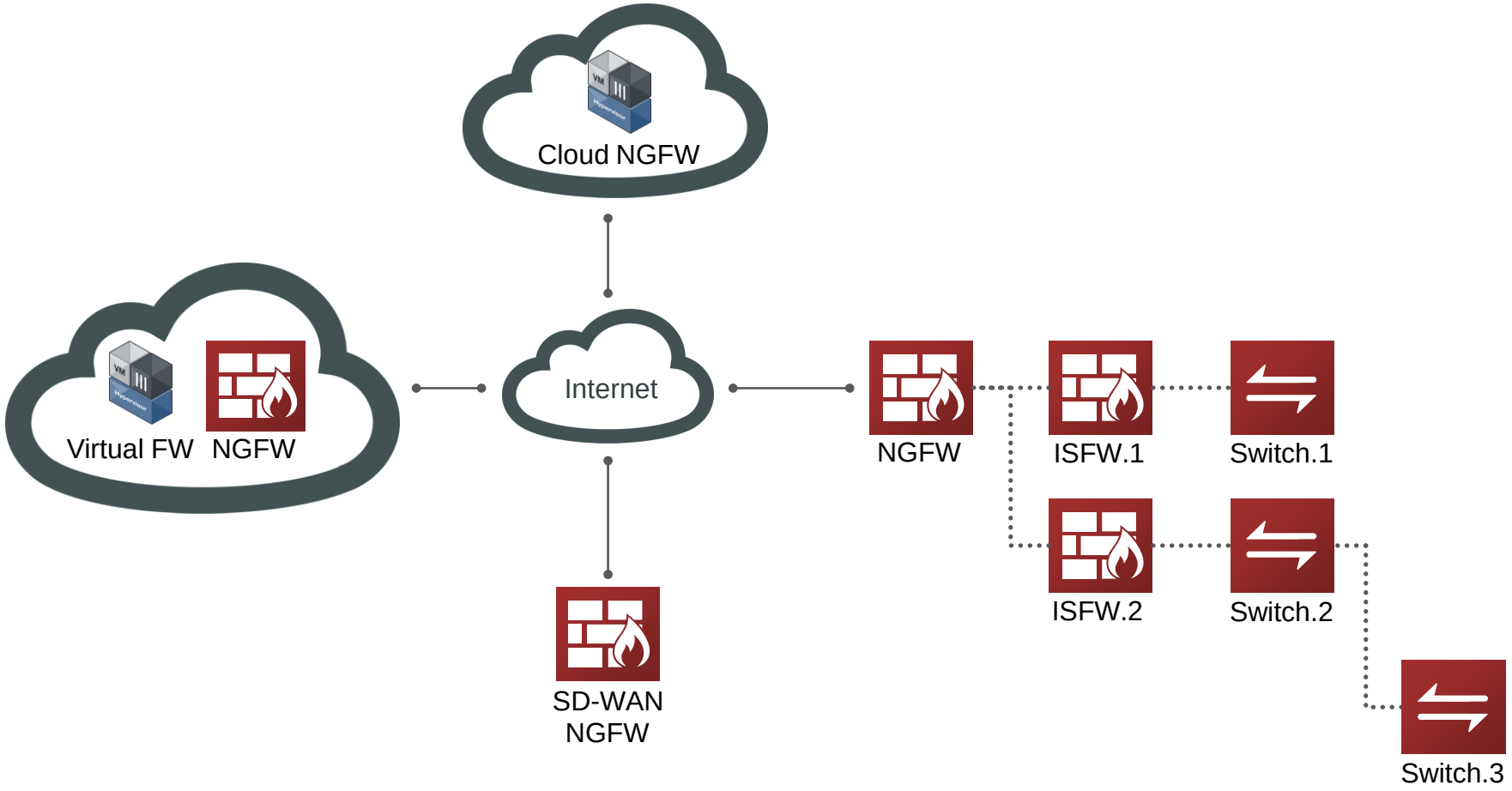


유무선 액세스 장비들 연결

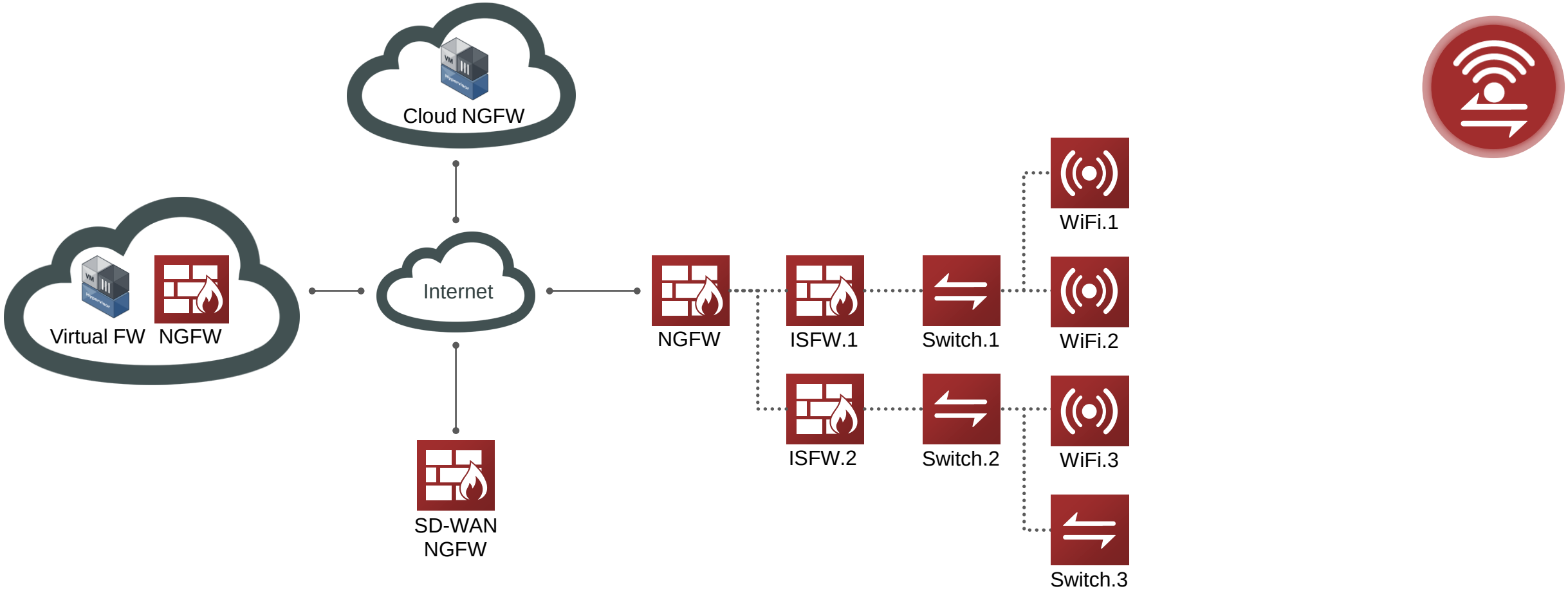
액세스 스위치

Wi-Fi 액세스 포인트

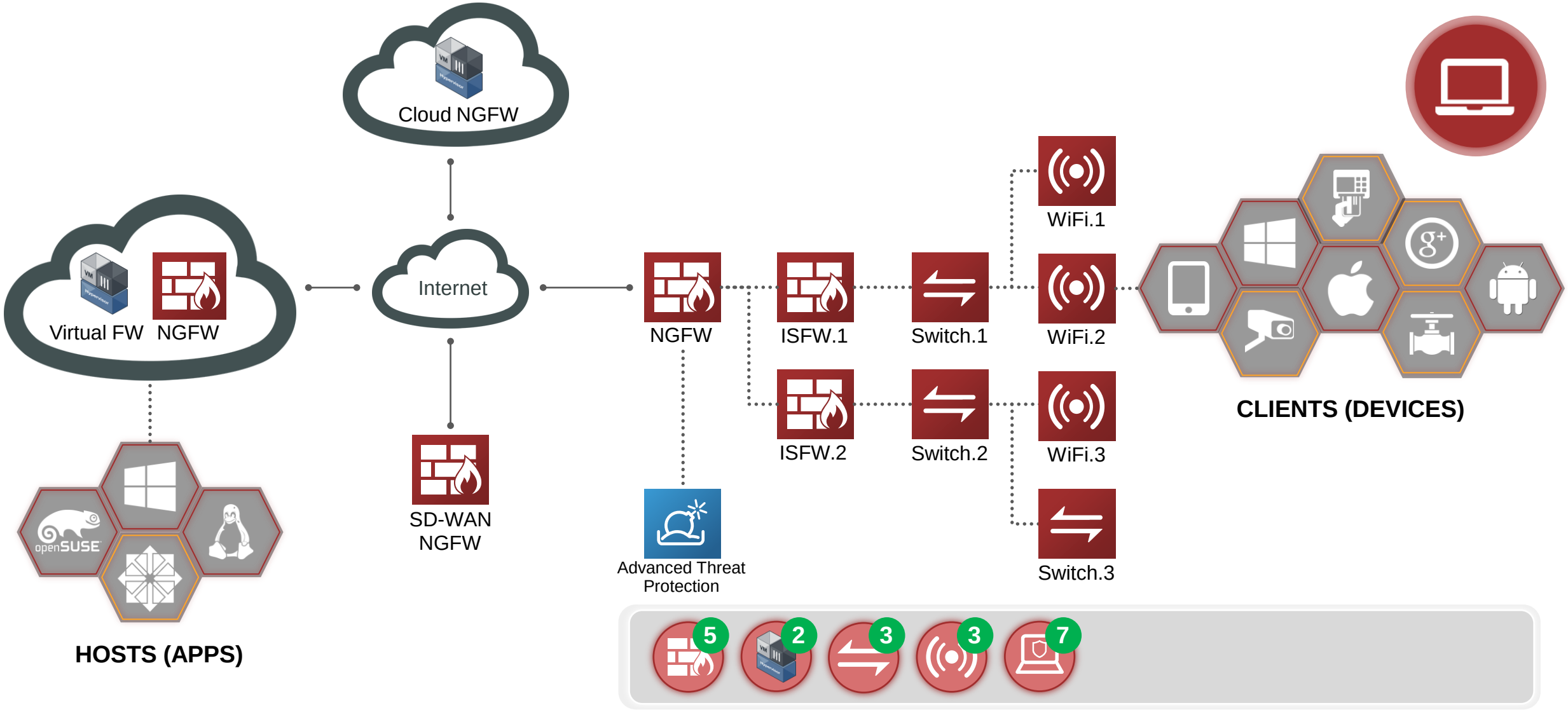
유무선 통합 보안 네트워크가 보이고 보호



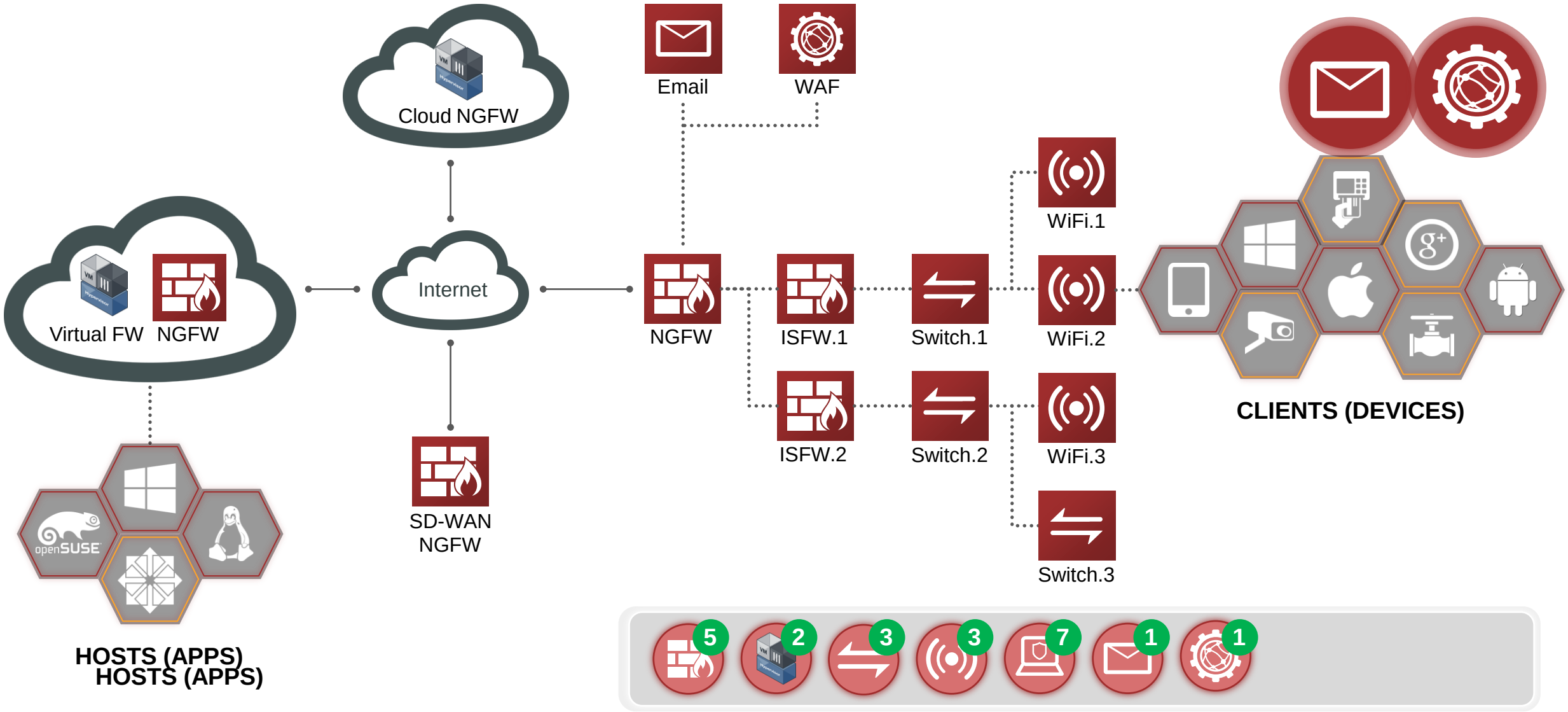
유무선 통합 보안 네트워크가 보이고 보호



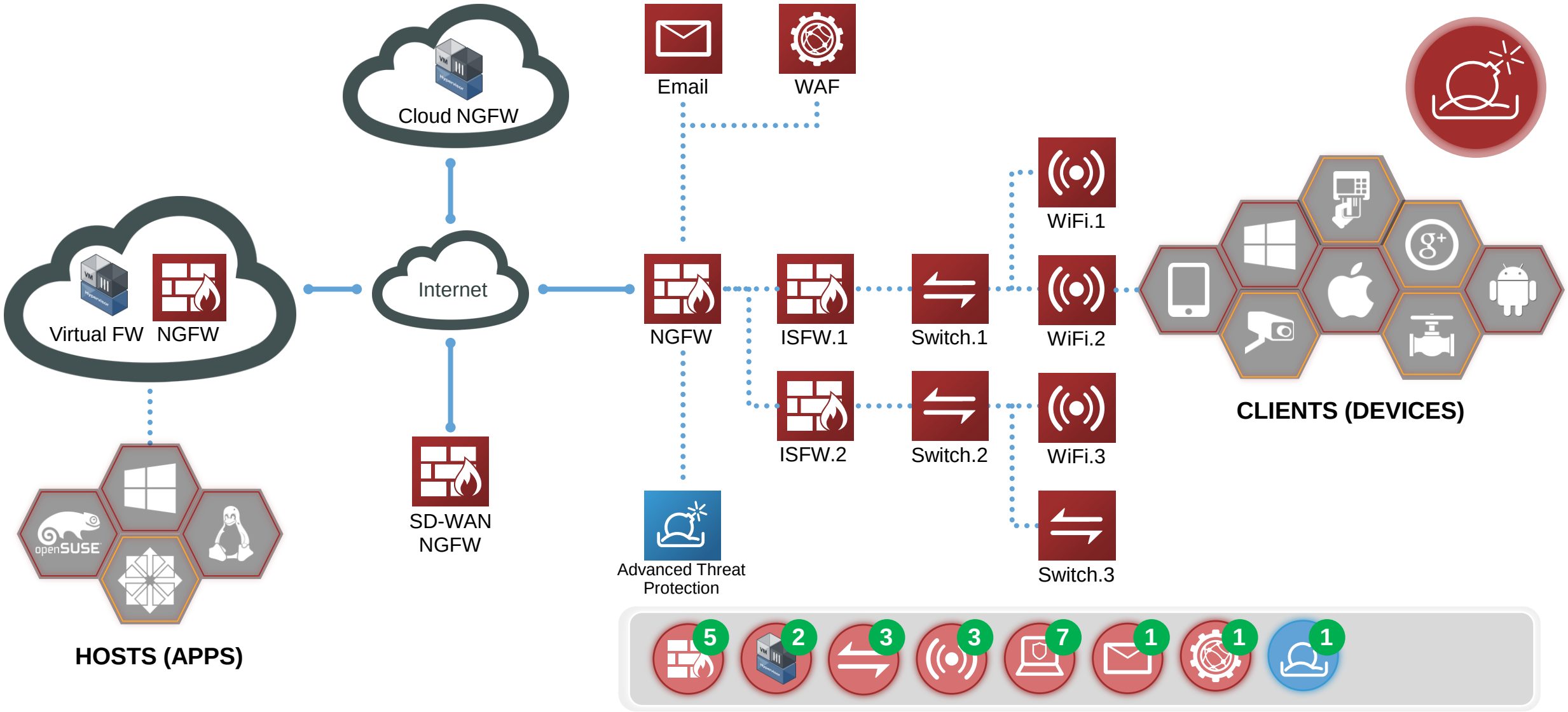
사용자 단말기 및 기기 등이 보이고 보호



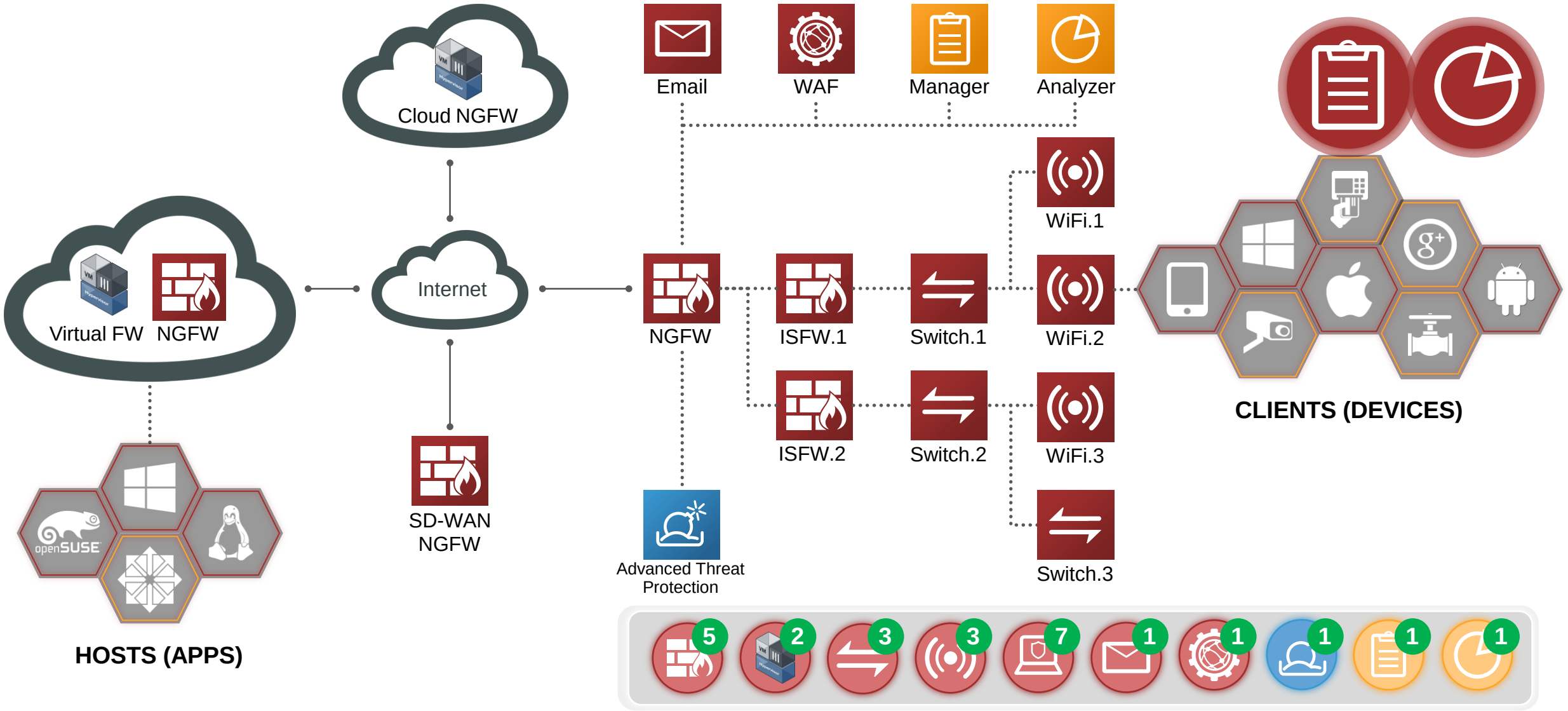
이메일, 웹 어플리케이션이 보이고 보호



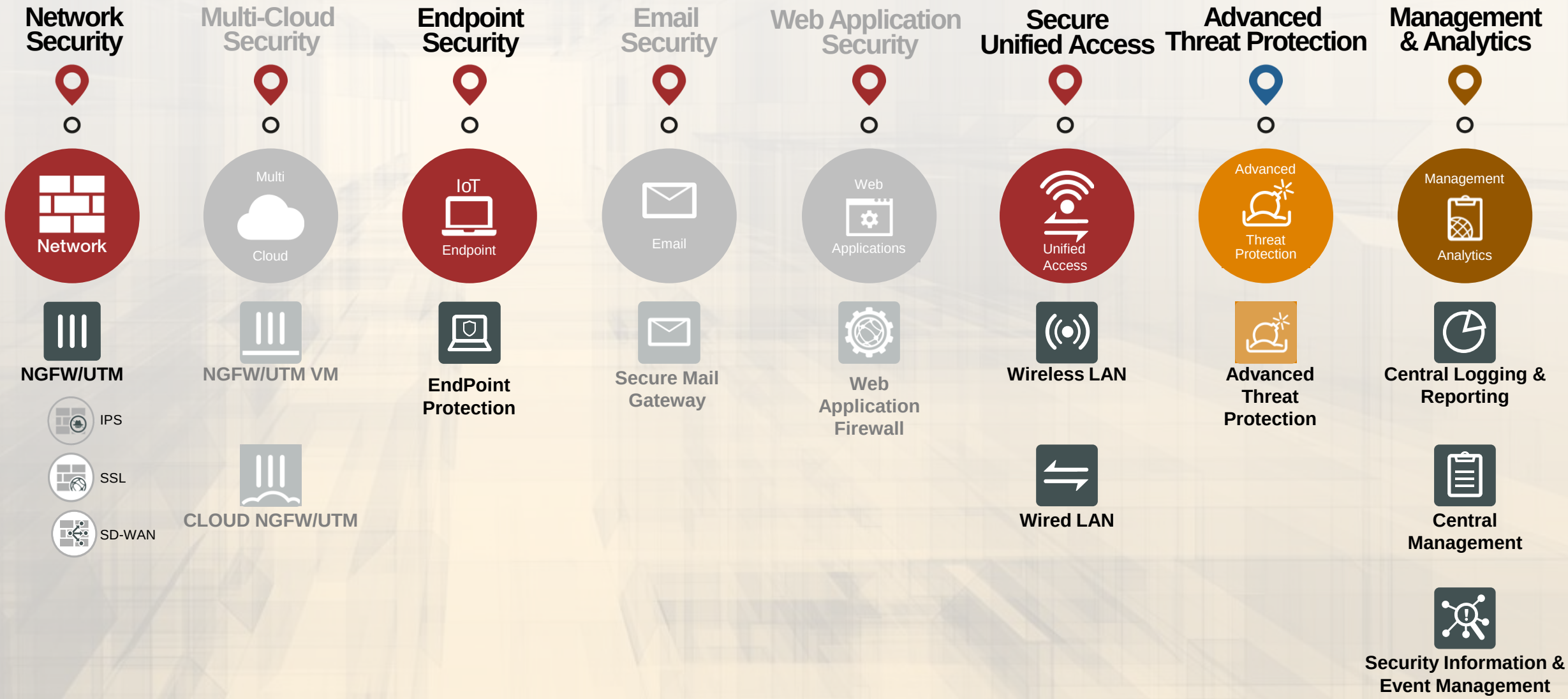
모든 패브릭 요소에서 지능형 탐지 기능을 사용



중앙관리 및 분석


Cloud NGFW
Email
WAF
Manager
Analyzer
Virtual FW
NGFW
Internet
WiFi.1
NGFW
ISFW.1
Switch.1
WiFi.2
ISFW.2
Switch.2
WiFi.3
SD-WAN
NGFW
Advanced Threat
Protection
Switch.3
CLIENTS (DEVICES)
HOSTS (APPS)
5
2
3
3
7
1
1
1
1
1

유무선 통합 보안 액세스 구성 요소

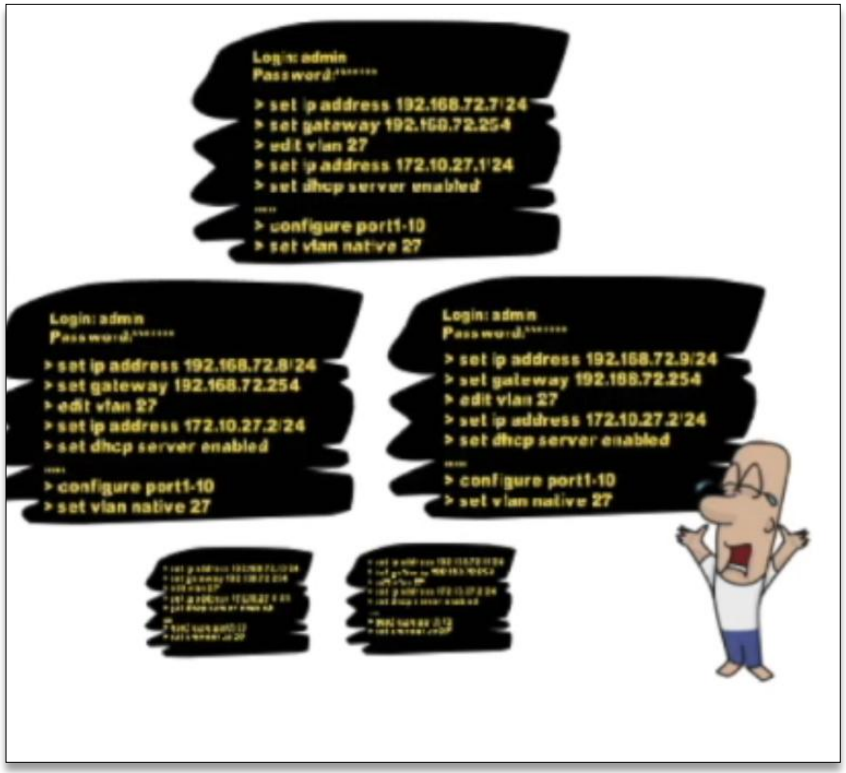


유무선 통합 보안 액세스 : 관리의 편의성

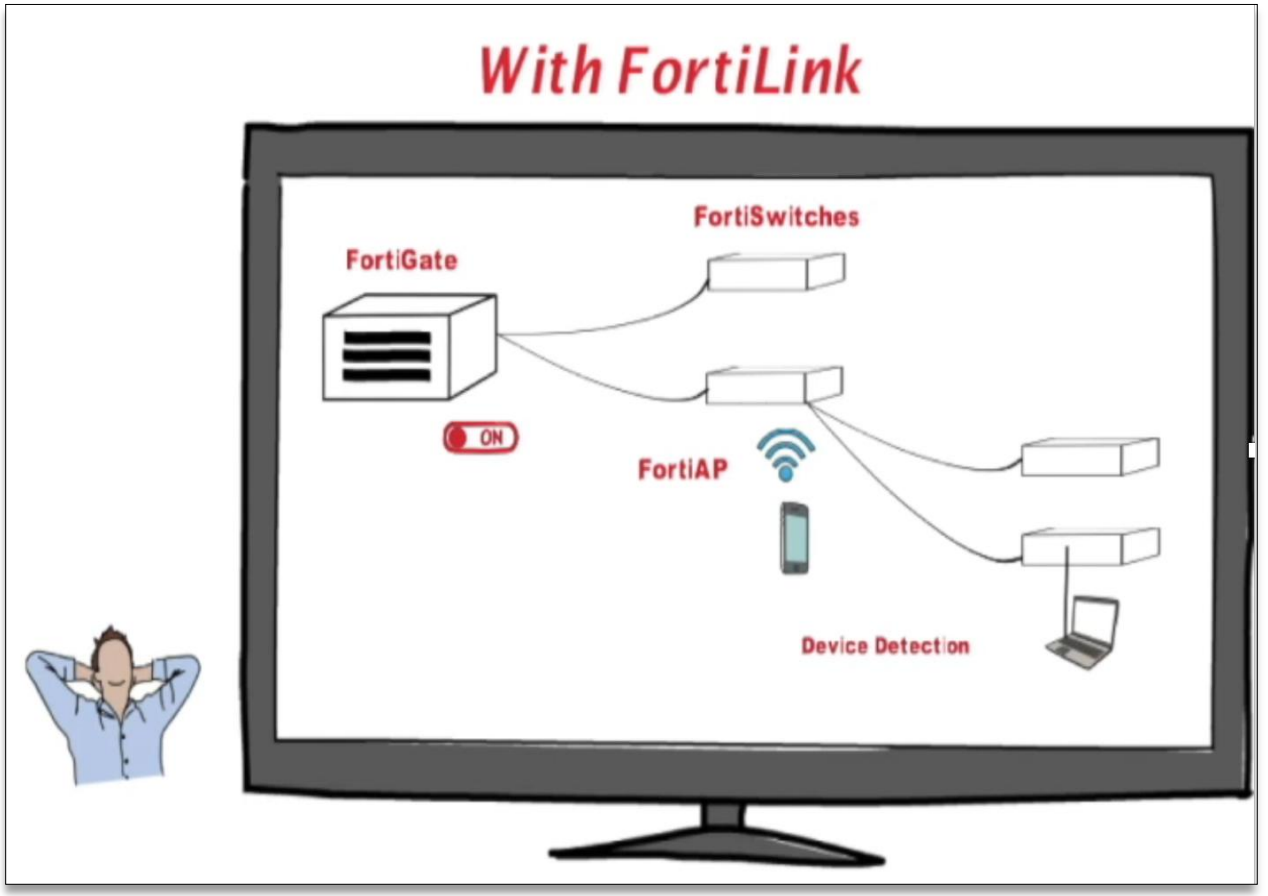
- 단일 창을 통해
  - 보안 정책
  - 스위치 관리/제어
  - 액세스 포인트 관리/제어
  - 사용자 제어
  - 트래픽 제어

인프라 구성의 간편화, 자동화

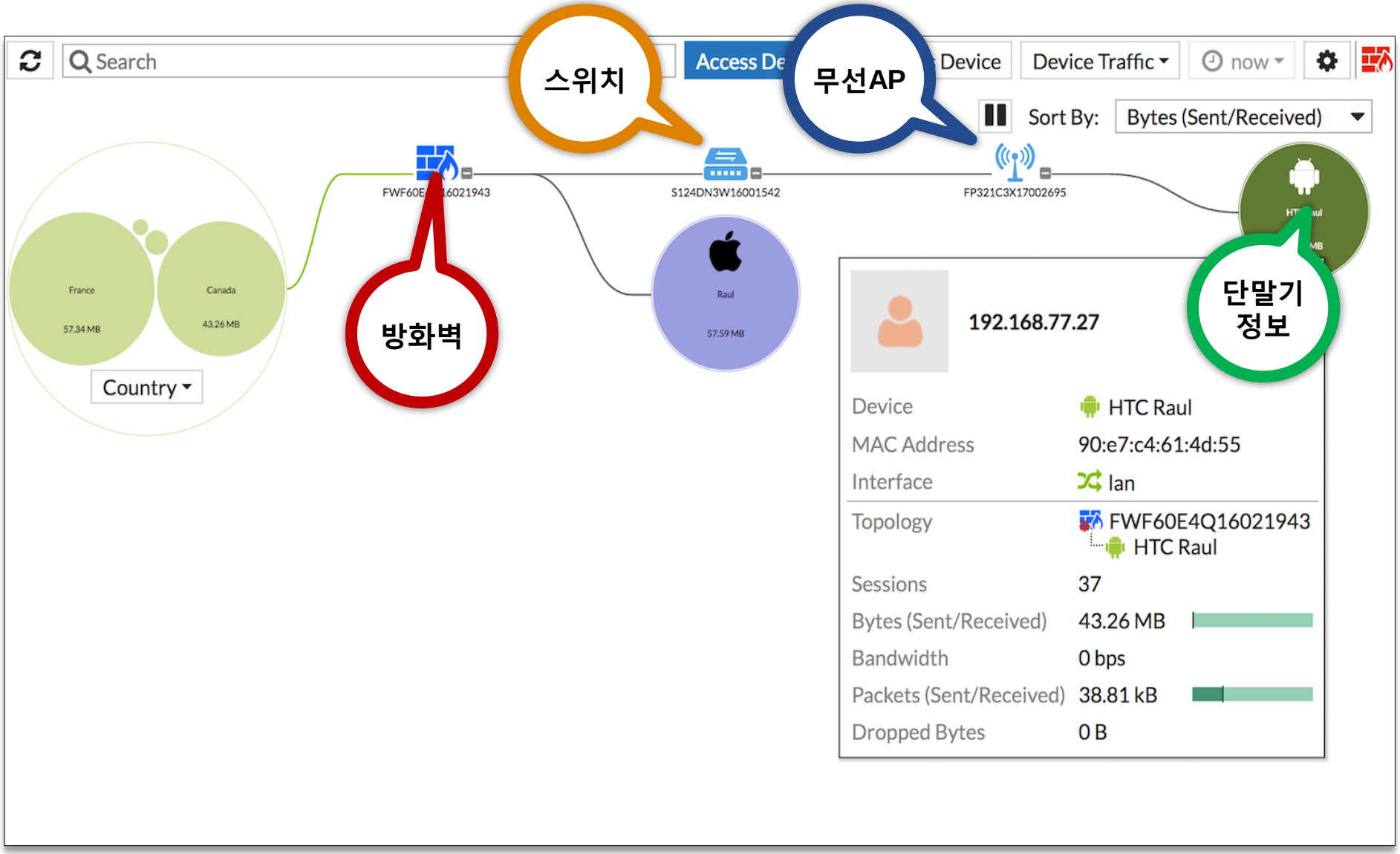
인프라 구성의 간편화, 자동화



VS

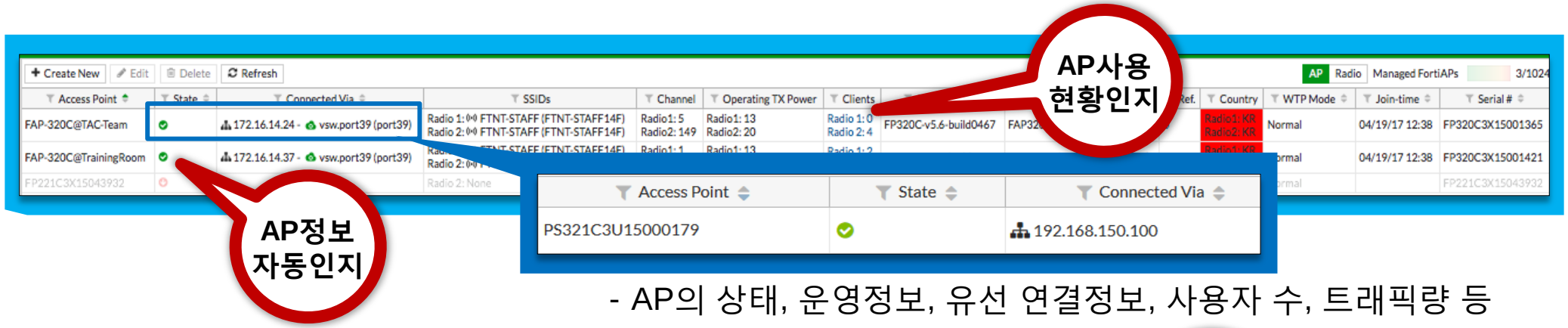


시큐리티 패브릭를 통한 전체 네트워크 관리

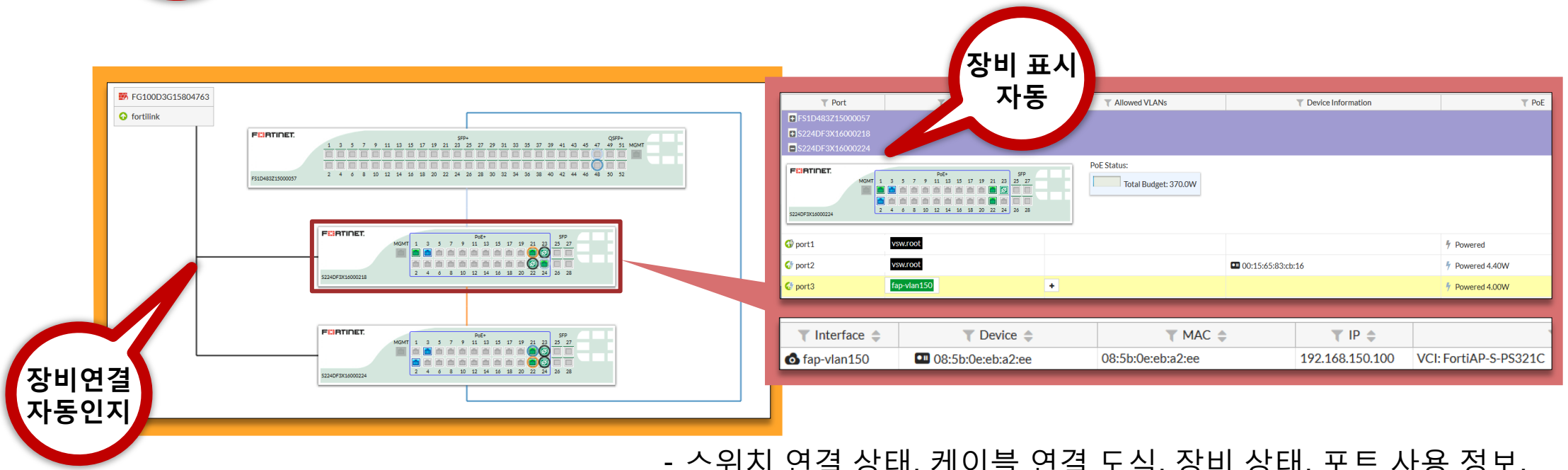


- 네트워크 토폴로지 파악
- 각 노드 별 장비 정보 표시
- 사용자, 트래픽, 세션 및 단말기 OS를 포함한 정보 표시
- 트래픽 및 세션 등이 증가하면 단말기의 아이콘 실시간 변화

유무선 컨트롤러를 통한 장비 통합 관리

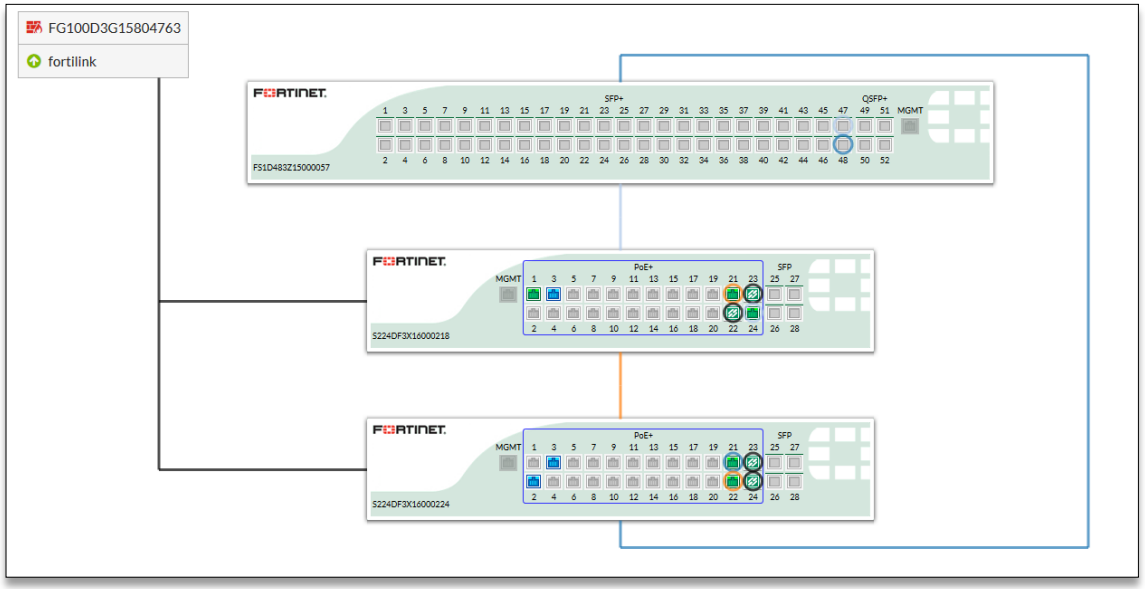


- AP의 상태, 운영정보, 유선 연결정보, 사용자 수, 트래픽량 등

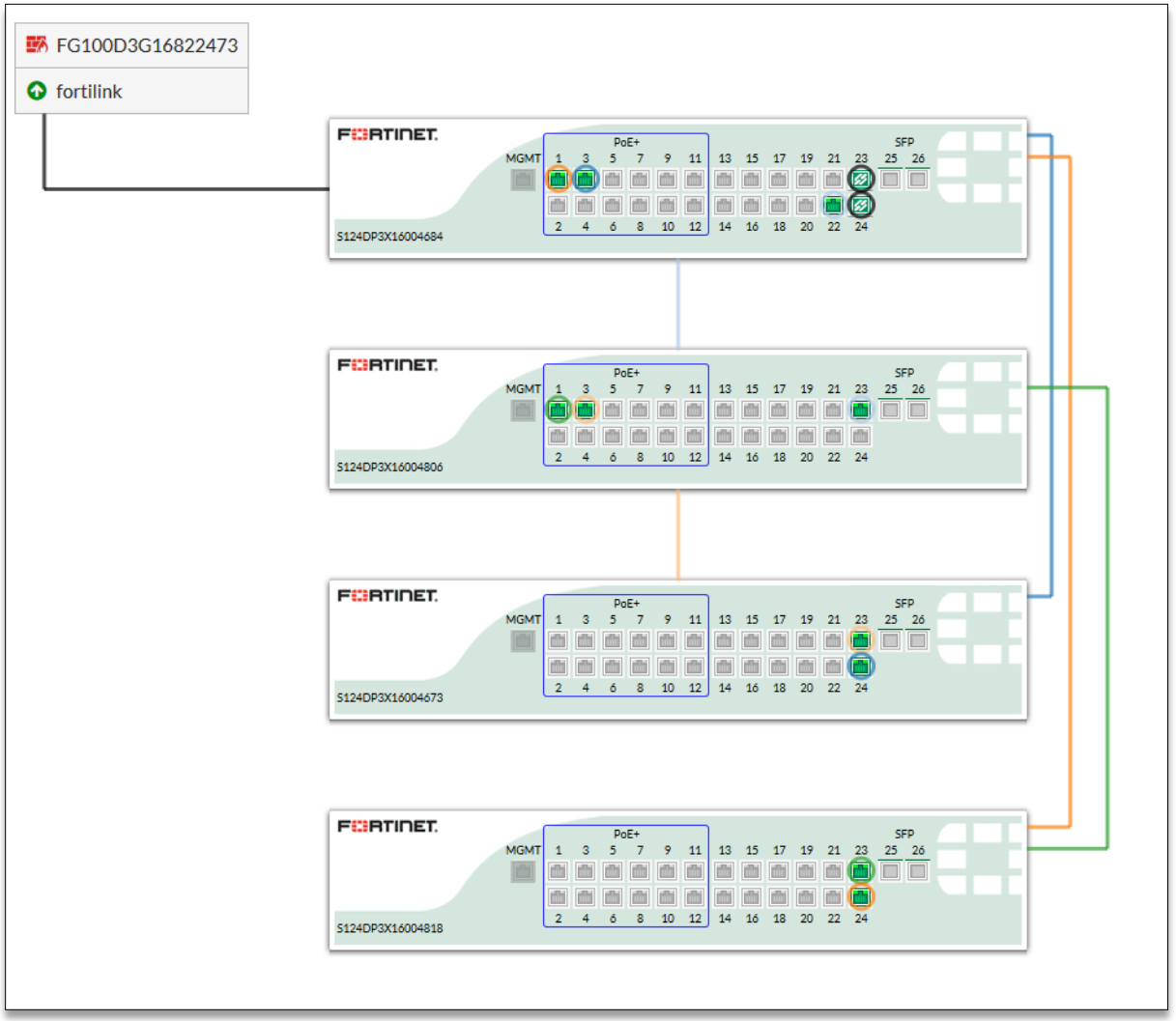


- 스위치 연결 상태, 케이블 연결 도식, 장비 상태, 포트 사용 정보, 포트 사용 주체 정보, 트래픽량 등

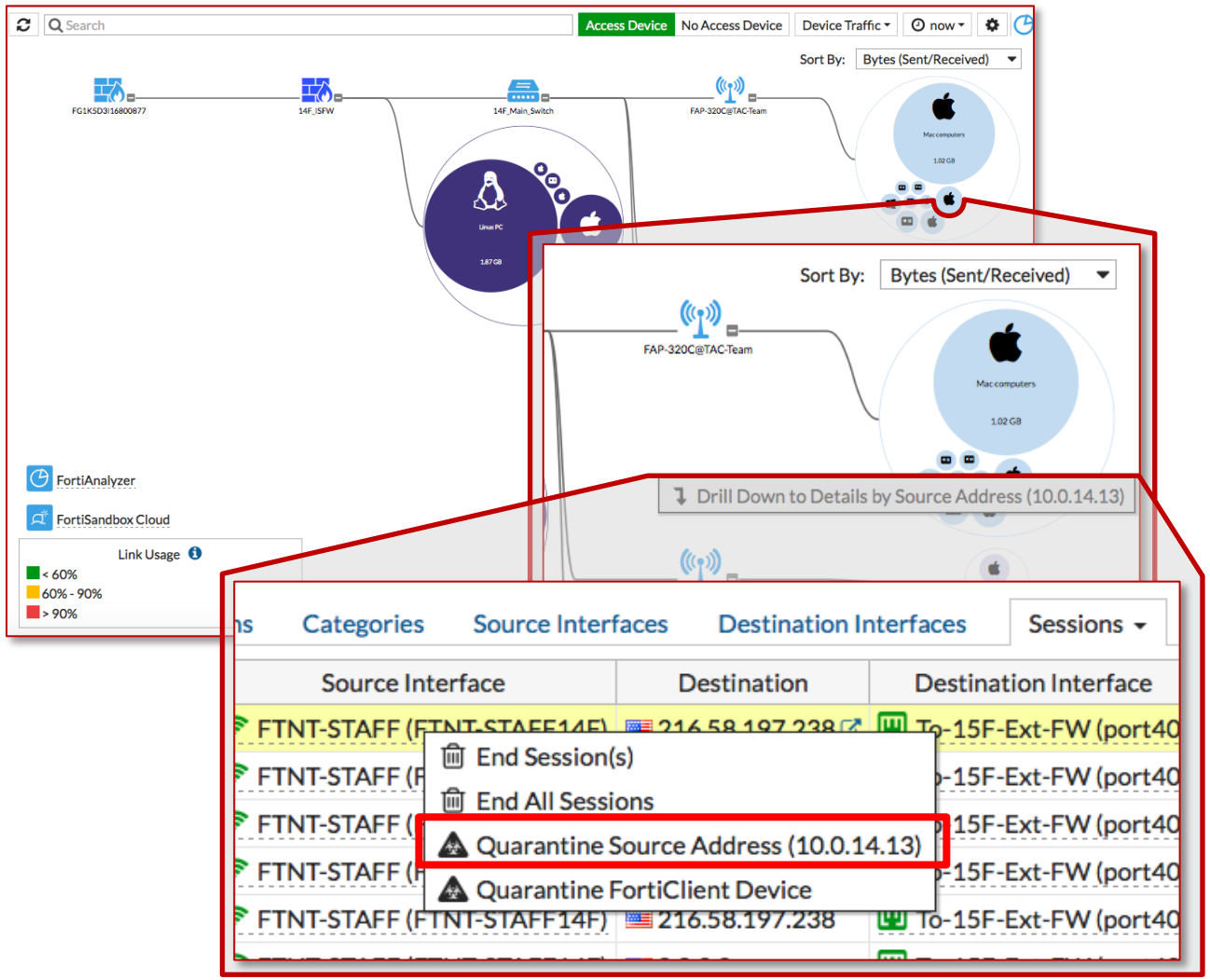
네트워크 토폴로지 자동 구성



- 스위치 연결을 위한 별도 설정 불필요
- 스위치 PLUG & PLAY 지원
- 스위치간 연결된 링크 자동 표시 및 인지
- 각 스위치간 연결 링크 인지



사용자 디바이스 확인, 분석 및 격리



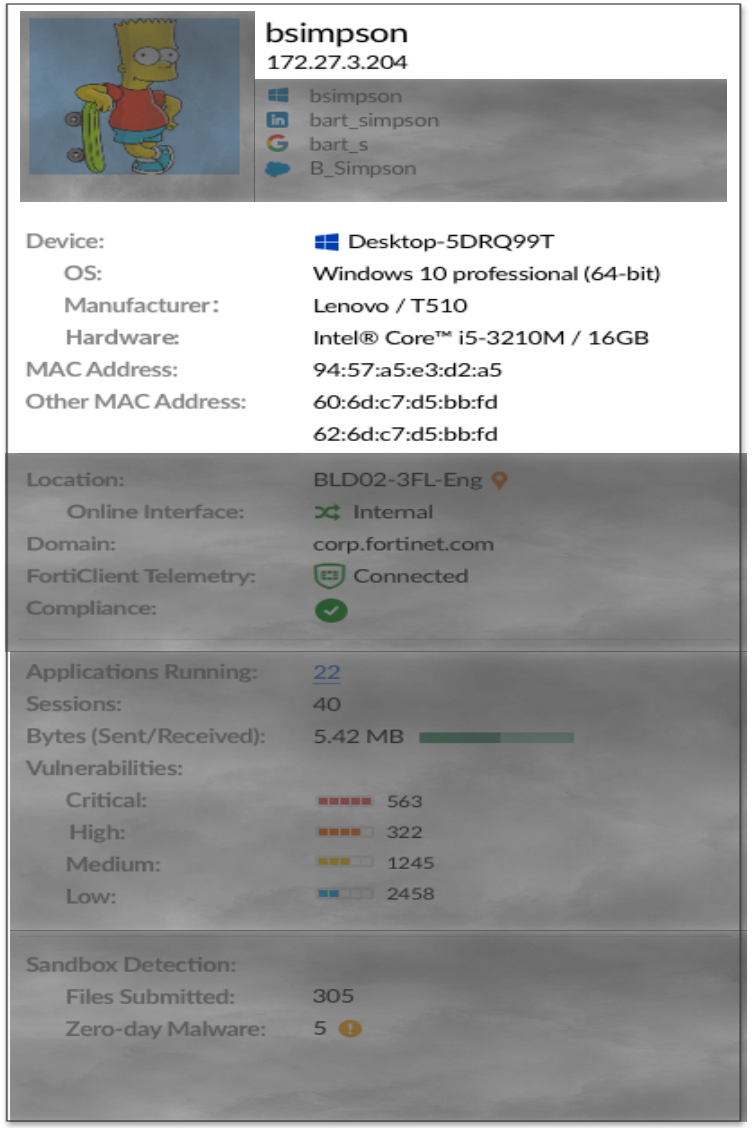
- 유무선 사용자 및 단말기에 대한 실시간 통합 모니터링
- 드릴다운 형식으로 사용자 상세 모니터링 가능
- 사용자가 사용중인 단말기 정보, 트래픽 이용 현황 등 모니터링
- 해당 단말기 및 사용자에 대해 보안 정책 적용

Endpoint Protection 도입 사용자 인지 및 통제

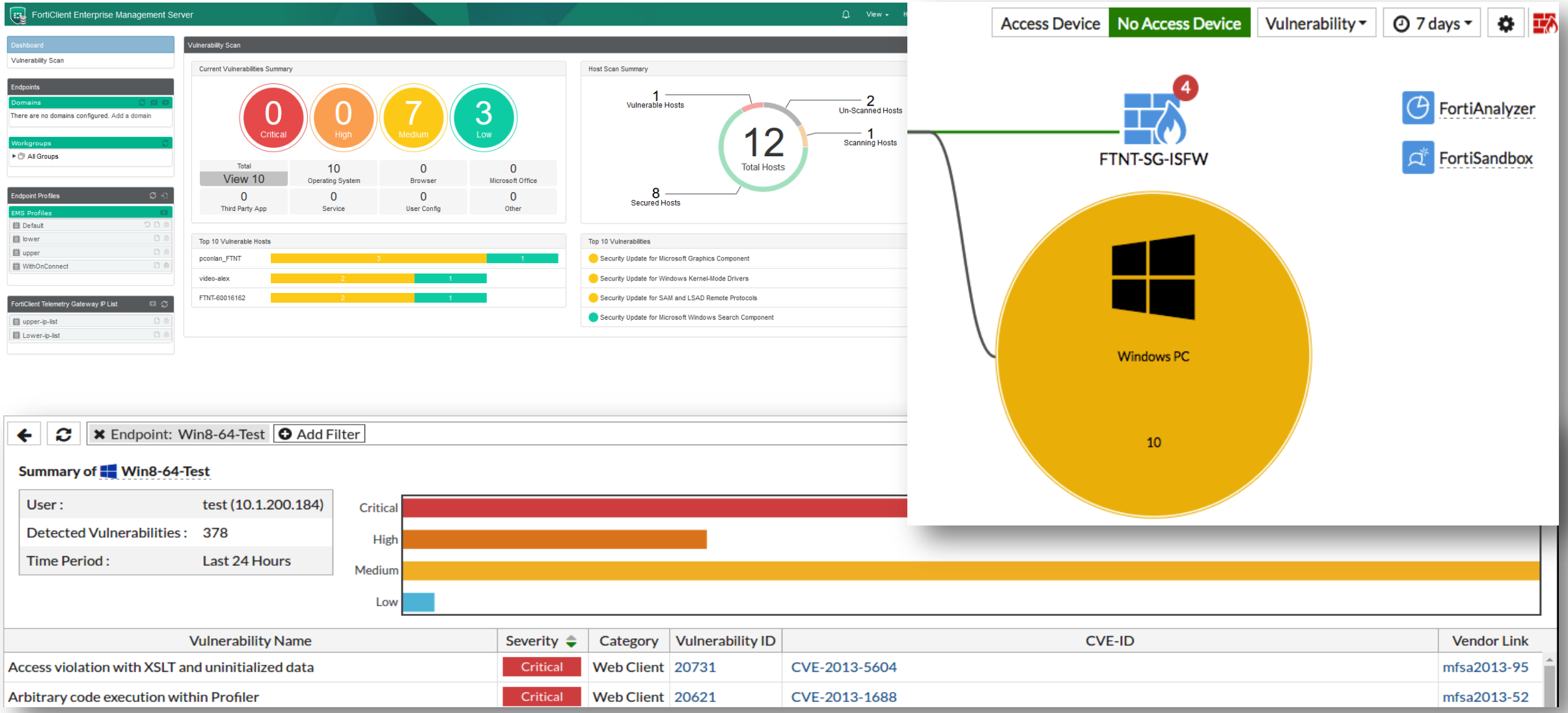
Endpoint S/W 설치 시, 최소 정보 내용

- 앤드포인트 텔레메트리
- 취약점 검색

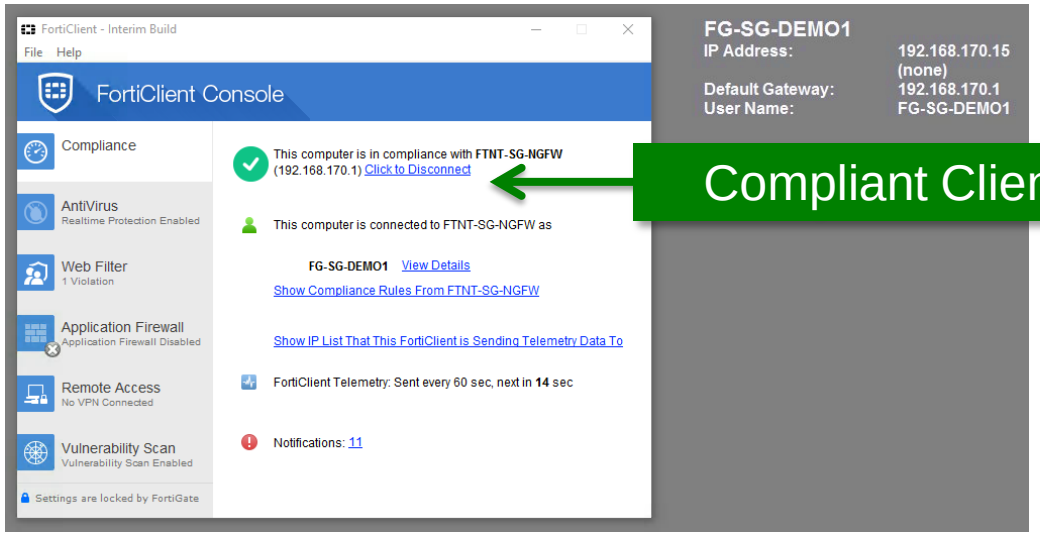
- **텔레메트리 데이터**
  - Avatars
  - Social IDs
- **규정준수**
  - Endpoint & configuration
- **취약점**
  - Vulnerability Scan & Report
  - Application Inventory



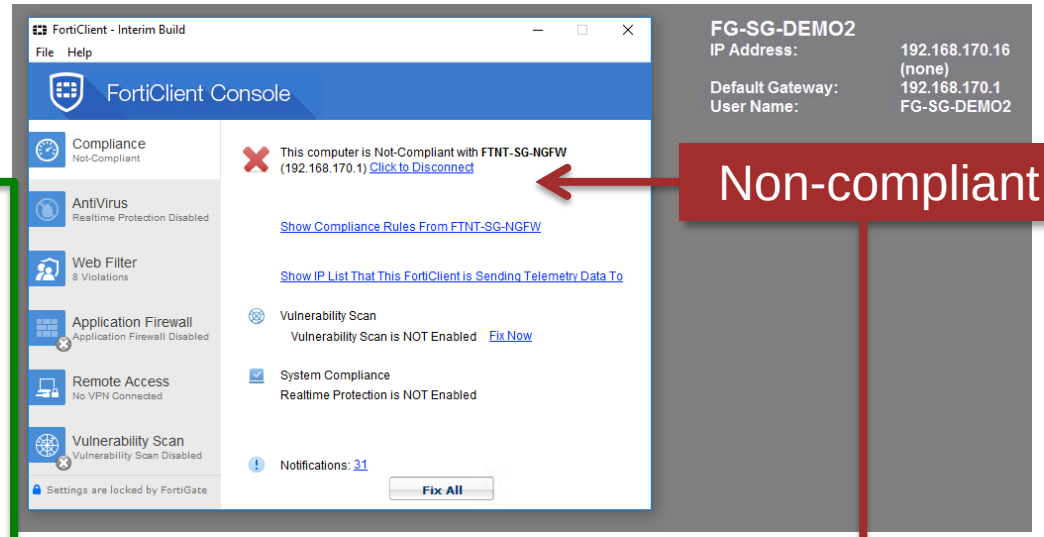
단말 취약점에 대한 네트워크 연계 및 보호



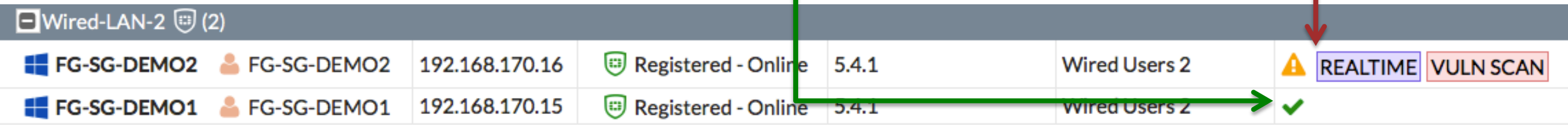
규정 준수, 취약 단말 패치 및 격리



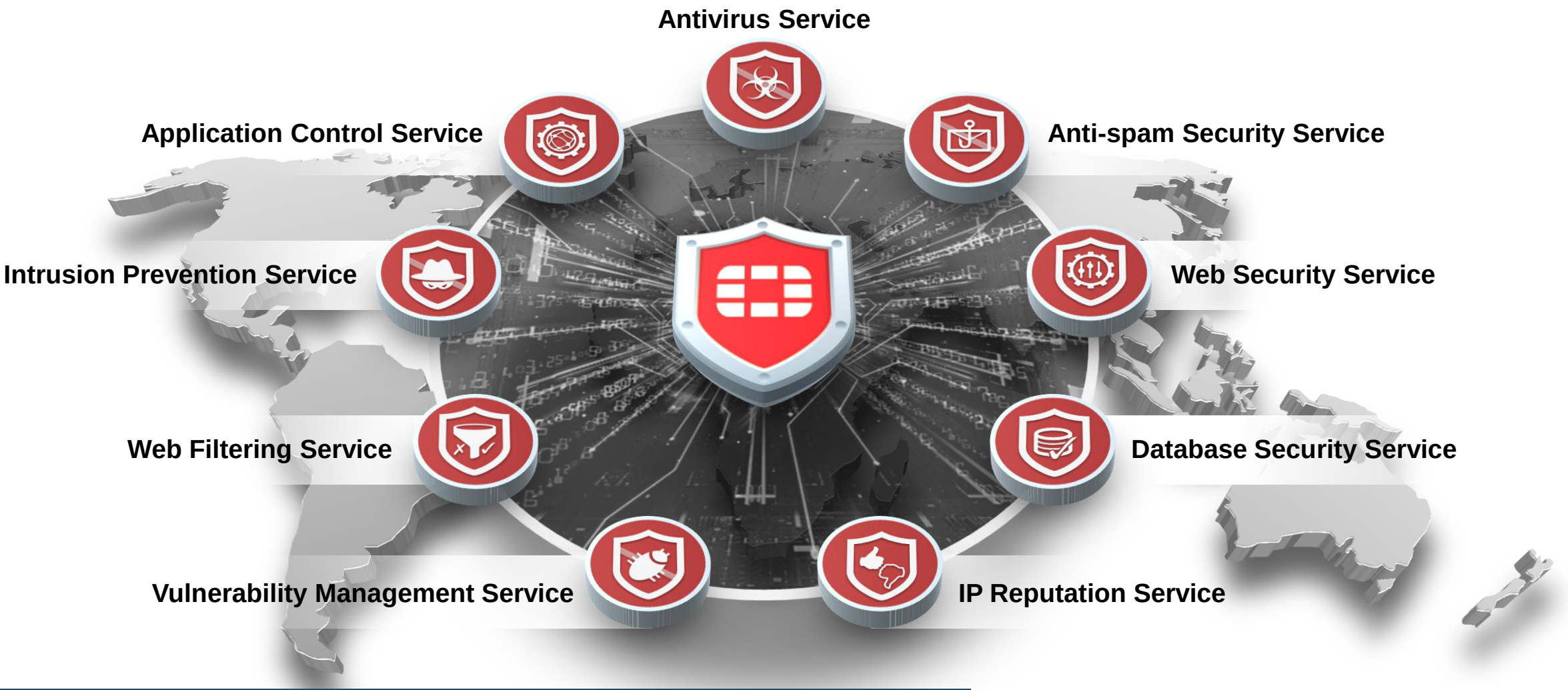
Compliant Client



Non-compliant Client



글로벌 위협 분석 DB 활용으로 다양한 보안 기능 제공



FNDN : Signature Lookup, Private Label, Threat Intel. Feed

차세대 UTM 방화벽 및 위협 방지를 넘어서...

Next Generation Firewall

VPN

Application Control

IPS

Web Filtering

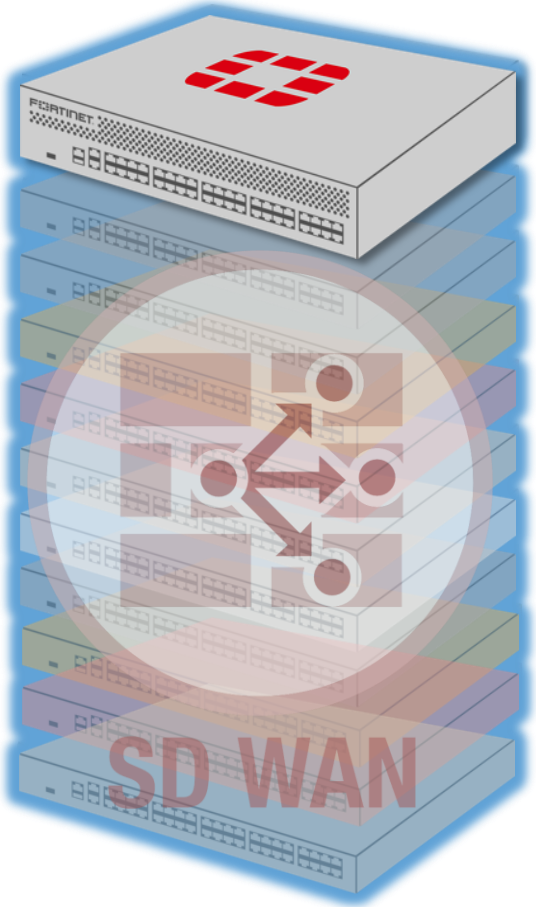
Anti-malware & Botnet

WAN Acceleration

Data Leakage Protection

Wi-Fi & Switch Controller

Advanced Threat Protection



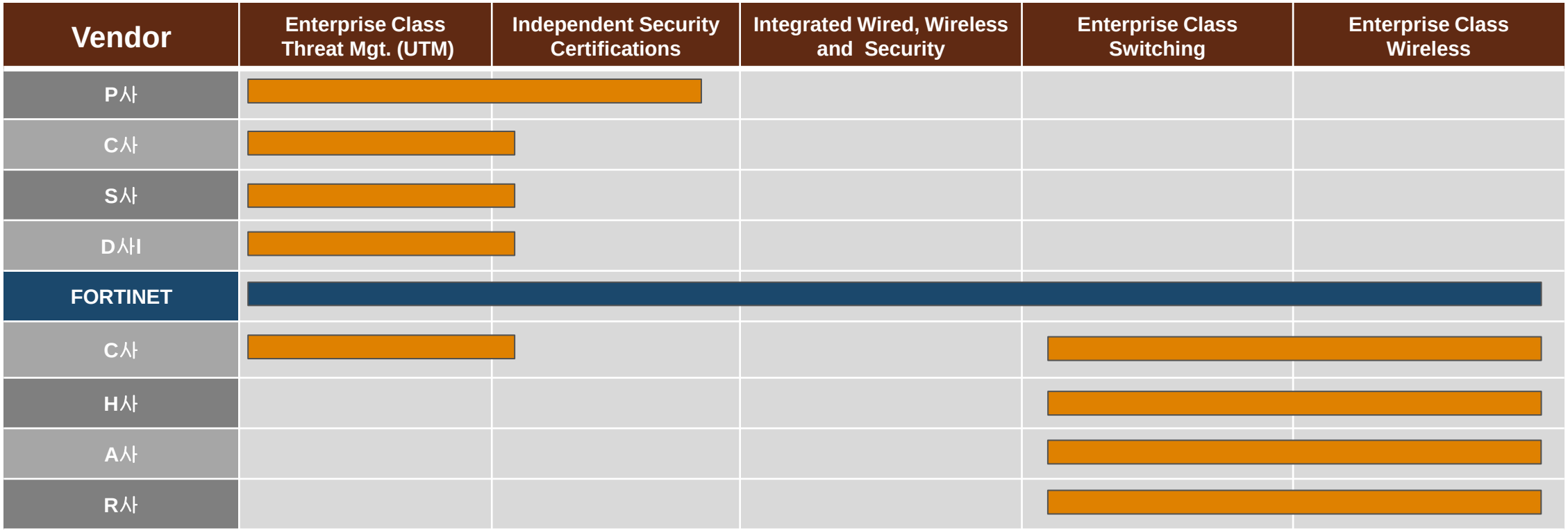
Secure SD-WAN

- 라우팅 및 VPN
- 링크 로드밸런싱
- 링크 품질 상태 점검
- 패킷 손실, 지연 및 지터 감지
- SaaS 기반 경로 선택

[UTM 기반 차세대 방화벽 보안 및 SD-WAN 통합]

포티넷의 유무선 통합 보안 액세스의 차별화

- 고성능 무선은 필수이나, 무선랜 서비스를 위해 이것만으로 충분하지 않음
- 강력한 스위칭은 필수이나, 통합 액세스를 위해 이것만으로 충분하지 않음
- 또한, 통합 위협 관리는 필수적이지만 독립형 솔루션은 아님
- 유무선 시큐어 액세스
- - 모든 네트워크 서비스 구현 및 배치에 대한 최소 요구 사항




FORTINET