제조업 고객사를 위한 포티넷 보안 솔루션 소개 웨비나

포티넷 코리아 SE팀 / 김기환

Q1, 2022

목차

1. 제조환경/ 공장에서 발생 가능한 보안 이슈

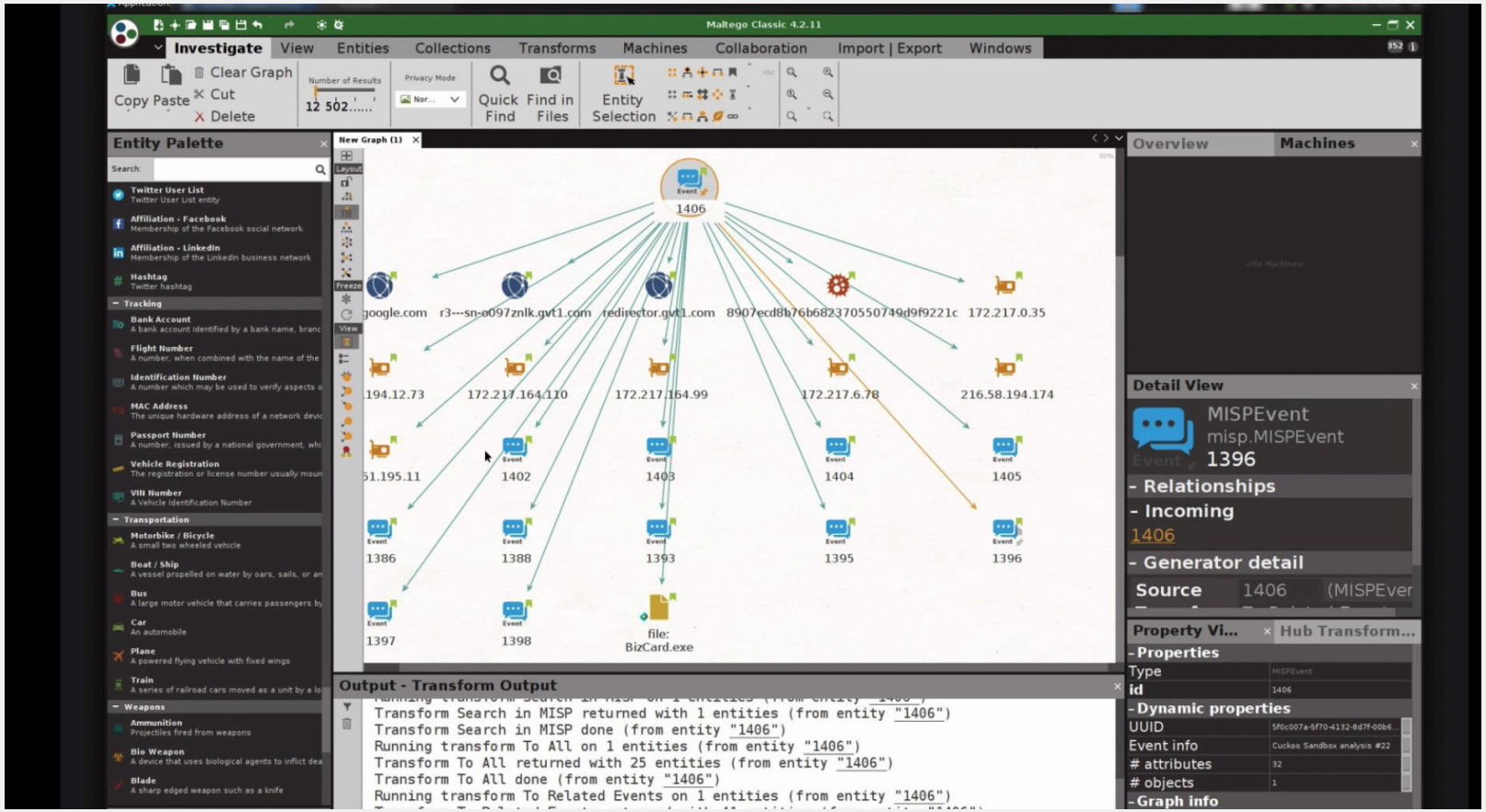
1. 제조환경/ 공장에서 발생 가능한 보안 이슈

동영상 별도 **Play**

1. 제조환경/ 공장에서 발생 가능한 보안 이슈

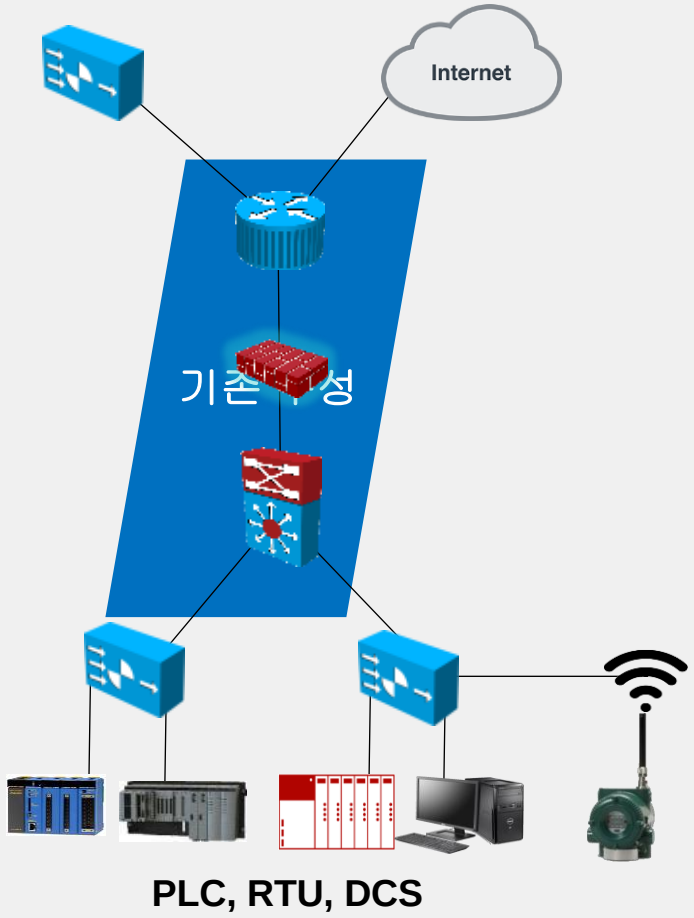
동영상 별도 **Play**

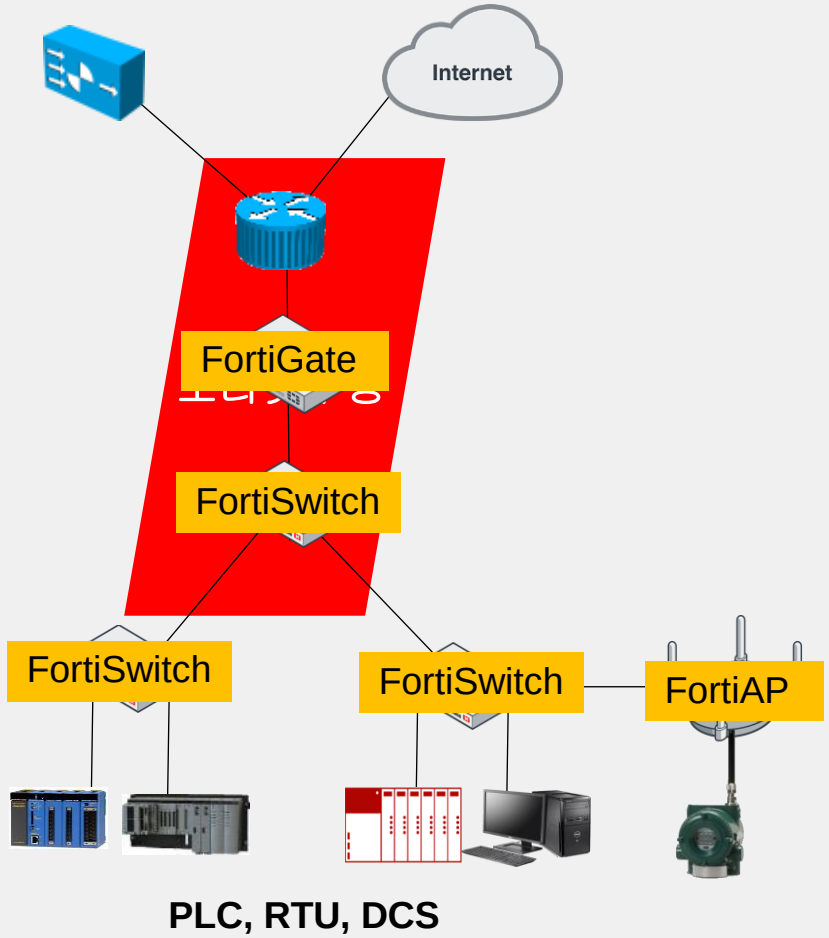
1. 제조환경/ 공장에서 발생 가능한 보안 이슈



2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

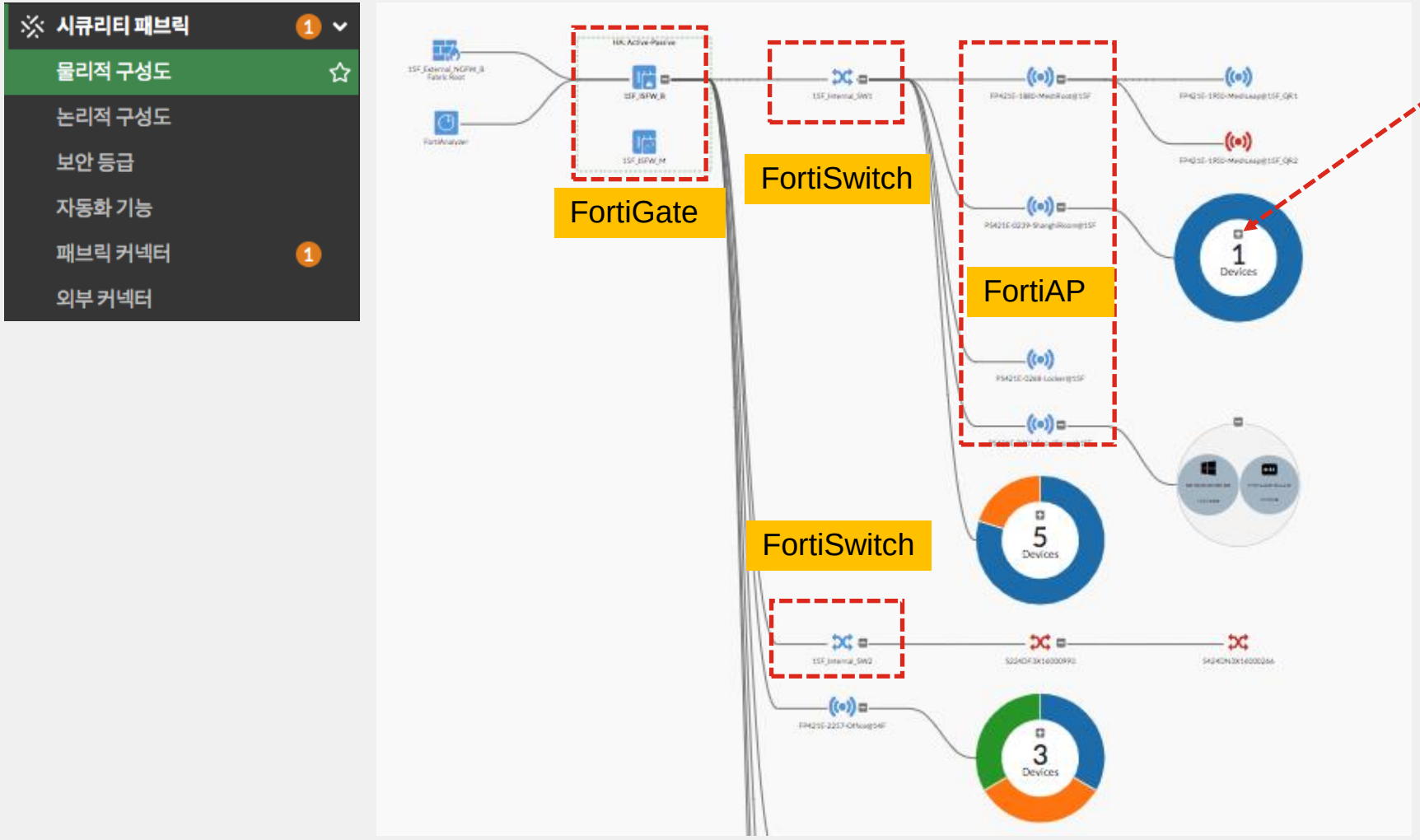
1)네트워크 인프라 가시성 확보 : FortiGate / FortiSwitch / FortiAP

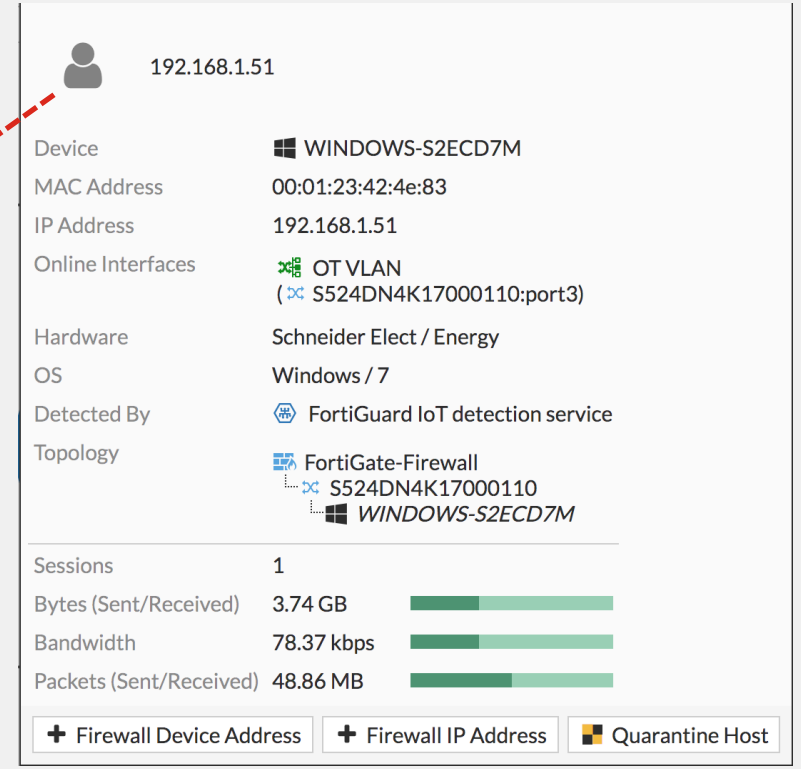




2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

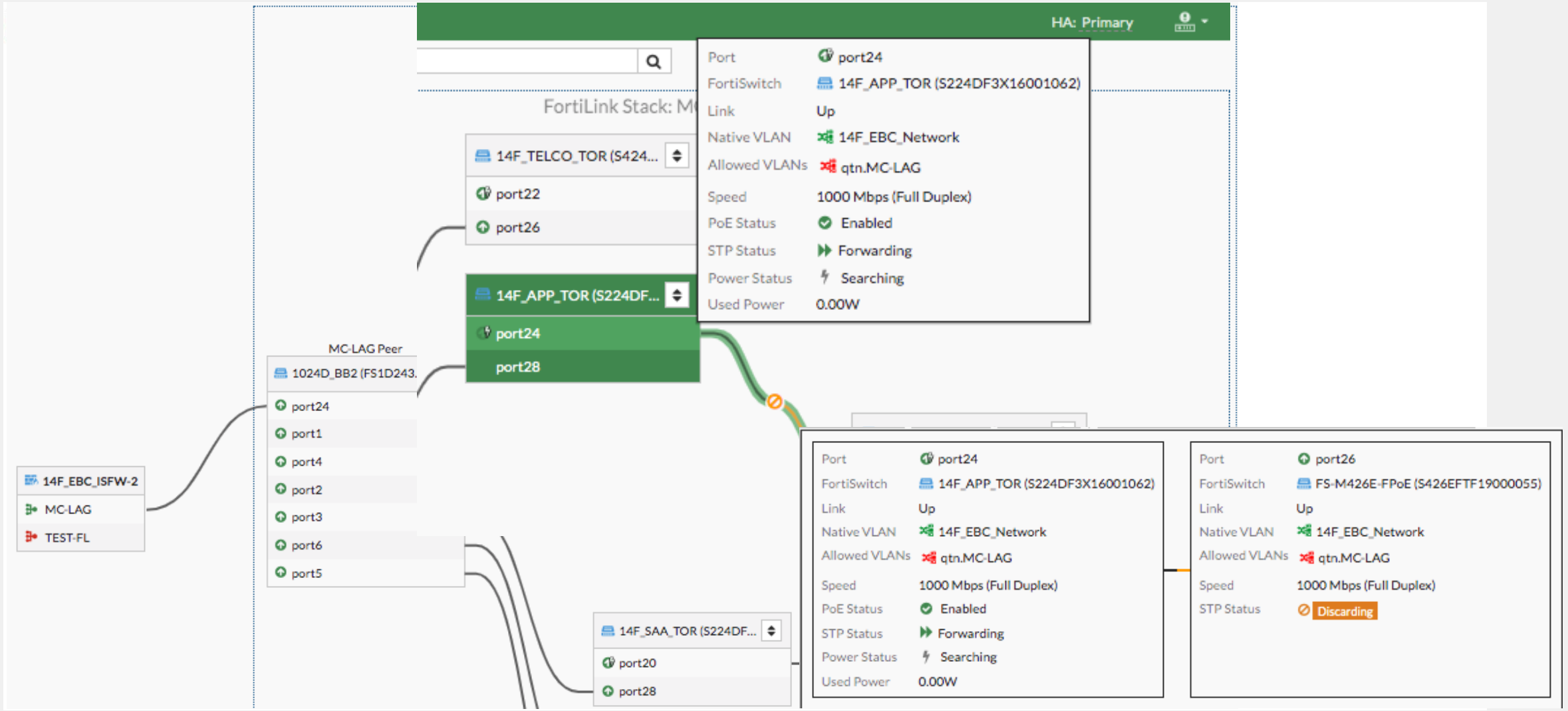
1)네트워크 인프라 가시성 확보 : FortiGate / FortiSwitch / FortiAP





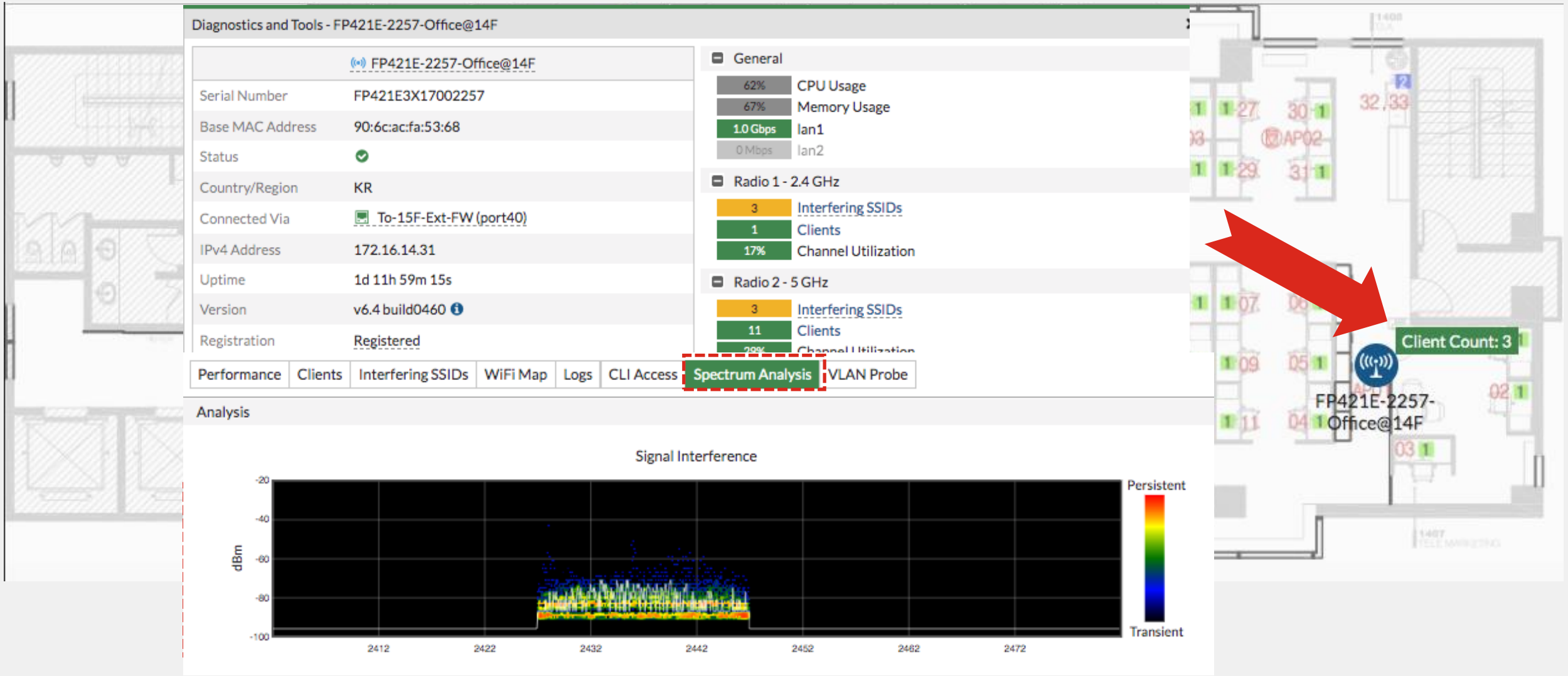
2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

1)네트워크 인프라 가시성 확보 : FortiGate / FortiSwitch / FortiAP



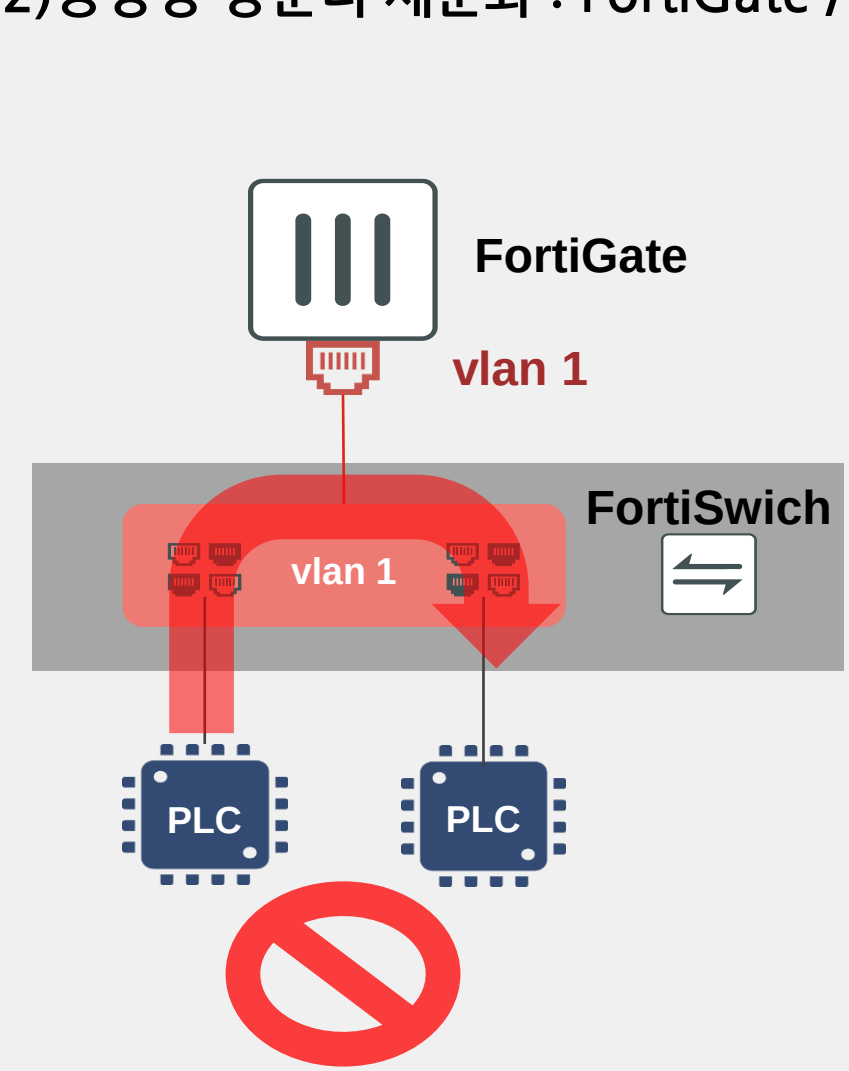
2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

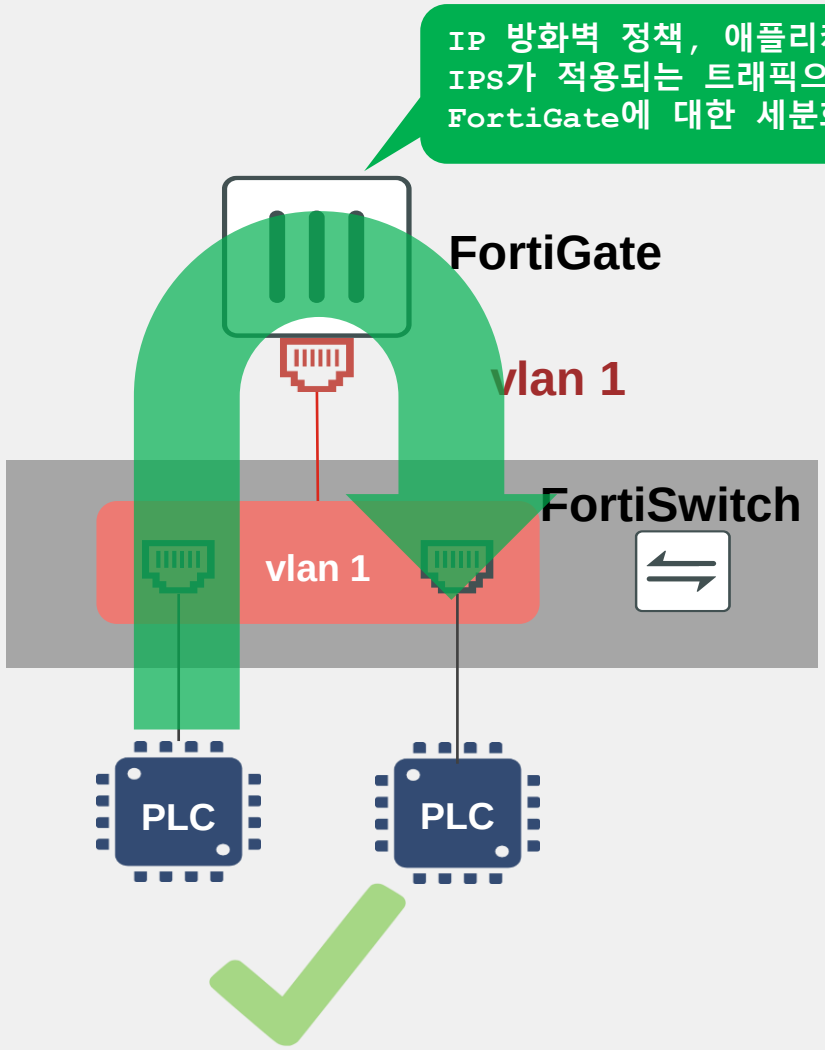
1)네트워크 인프라 가시성 확보 : FortiGate / FortiSwitch / FortiAP



2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

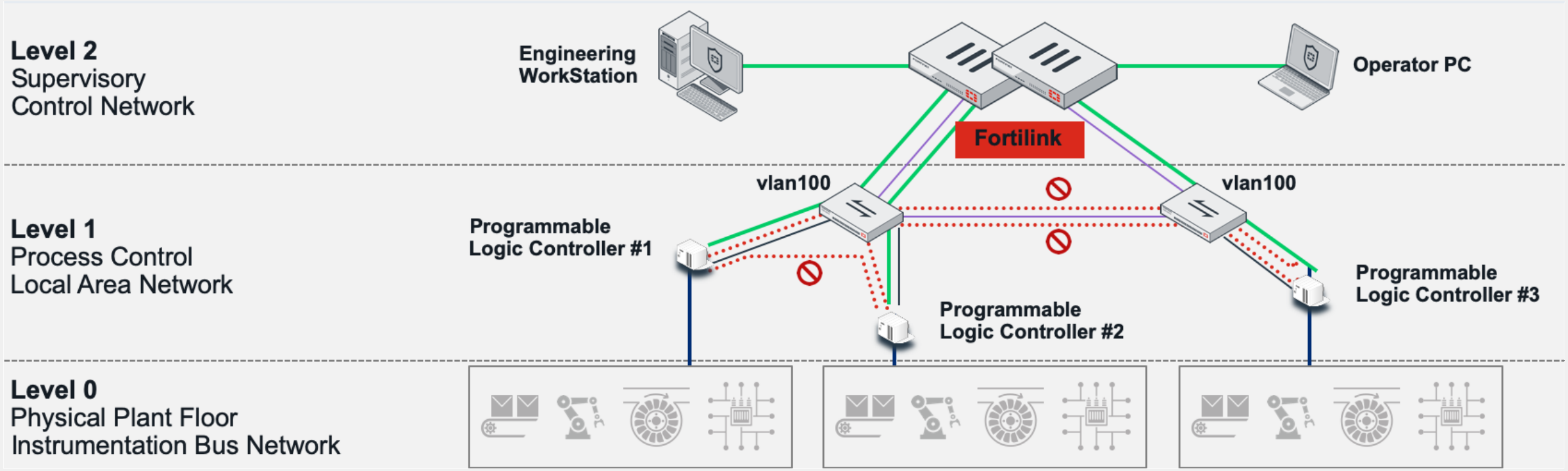
2)공장망 망분리 세분화 : FortiGate / FortiSwitch





2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

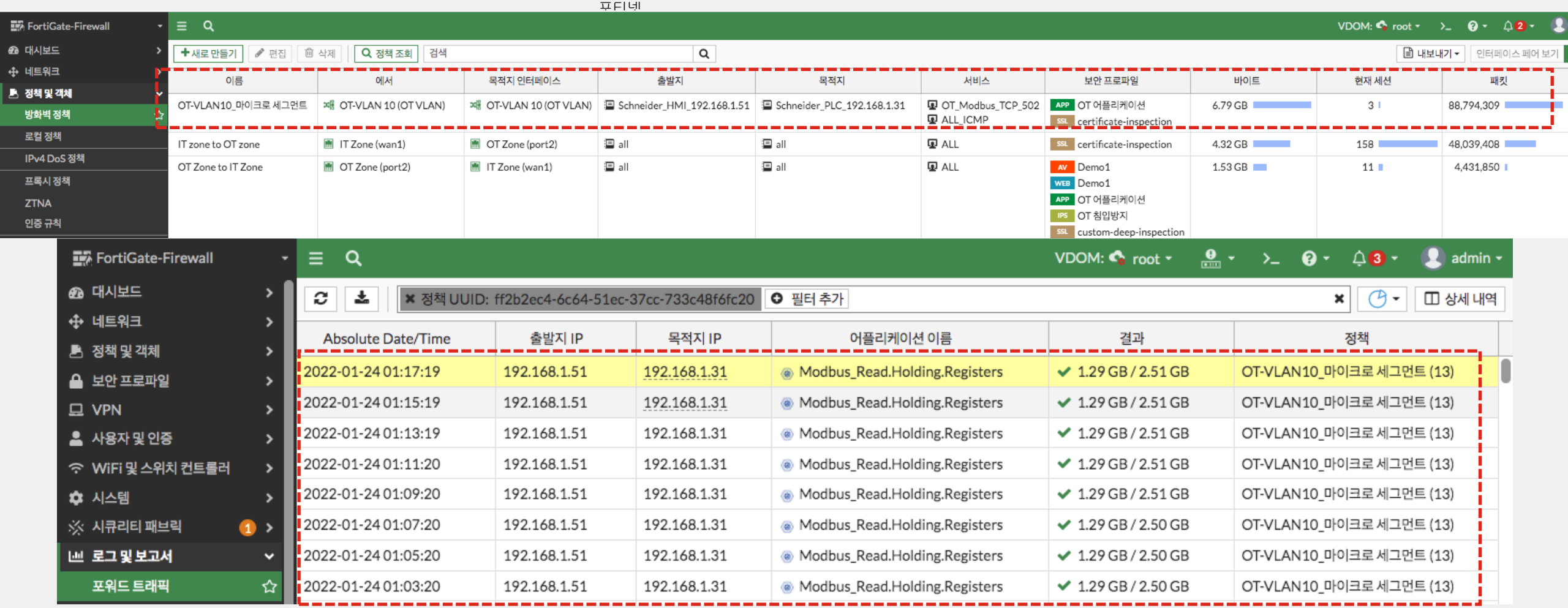
2)공장망 망분리 세분화 : FortiGate / FortiSwitch



2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

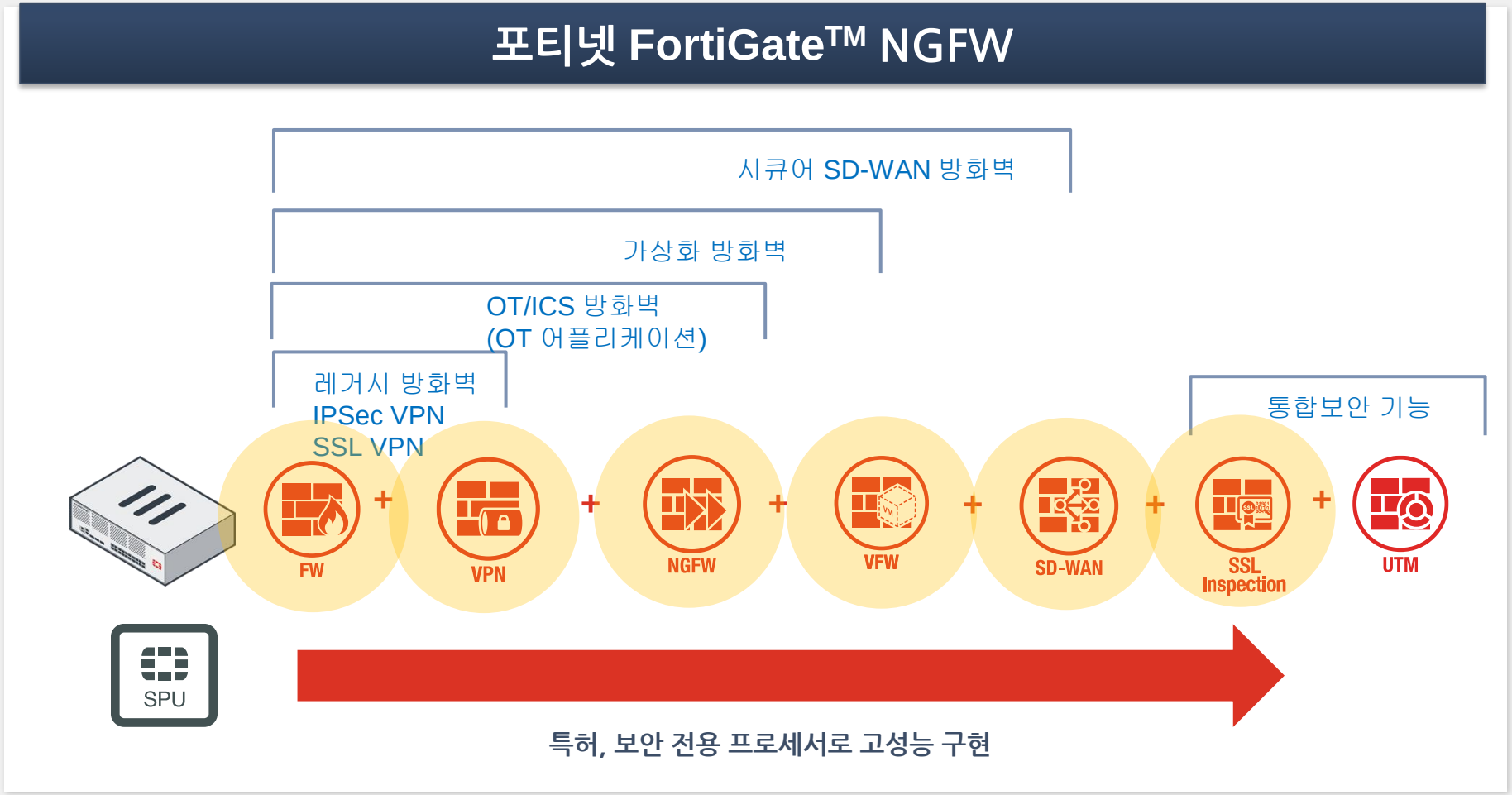
2)공장망 망분리 세분화 : FortiGate / FortiSwitch

포티넷



2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

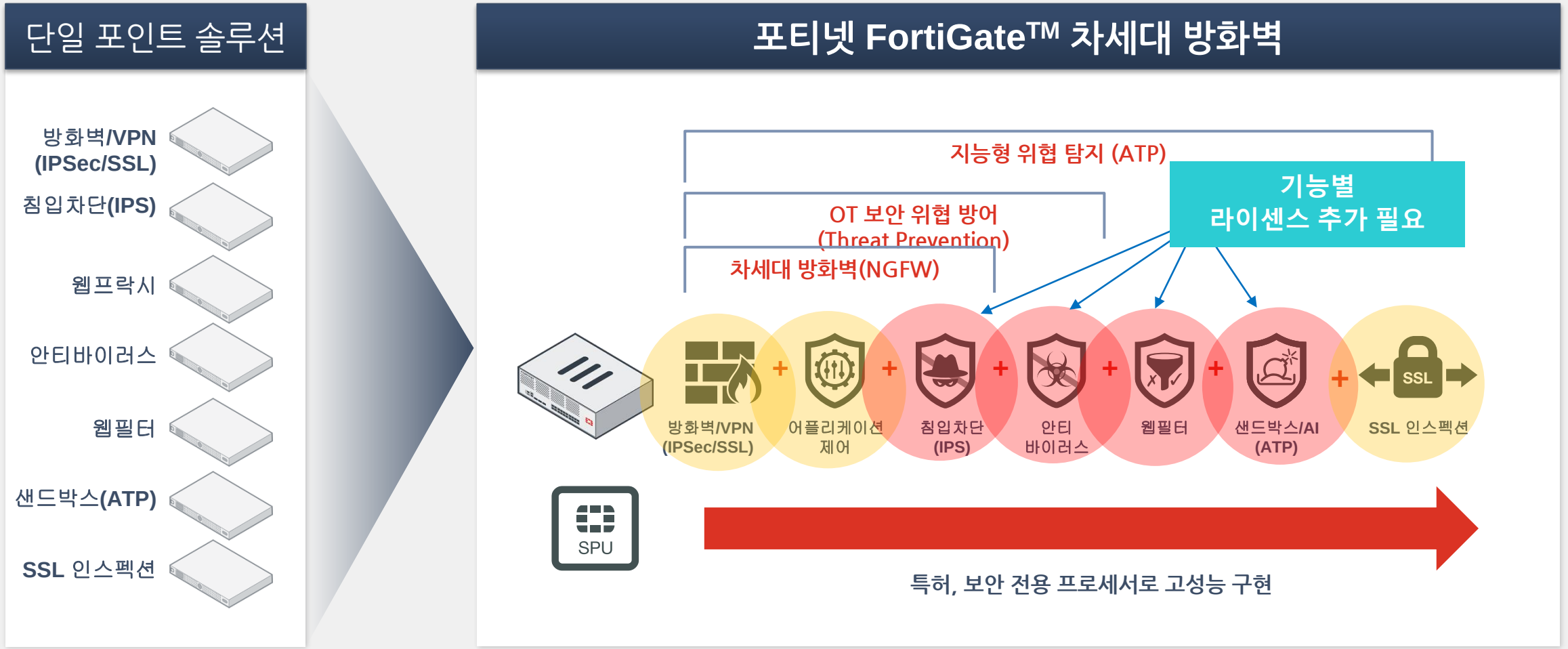
3)네트워크 트래픽 통제 : FortiGate NGFW(UTM)



- 제조환경/ 공장 인프라환경에 필요한 기능이 포티넷 FortiGate 방화벽에 통합

2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

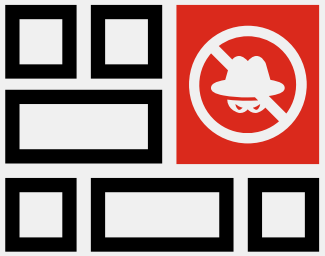
3)네트워크 트래픽 통제 : FortiGate NGFW(UTM)



- 단일 포인트 솔루션 기능이 FortiGate NGFW(차세대 방화벽) 기능에 통합

2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

3)네트워크 트래픽 통제 : FortiGate NGFW(UTM)



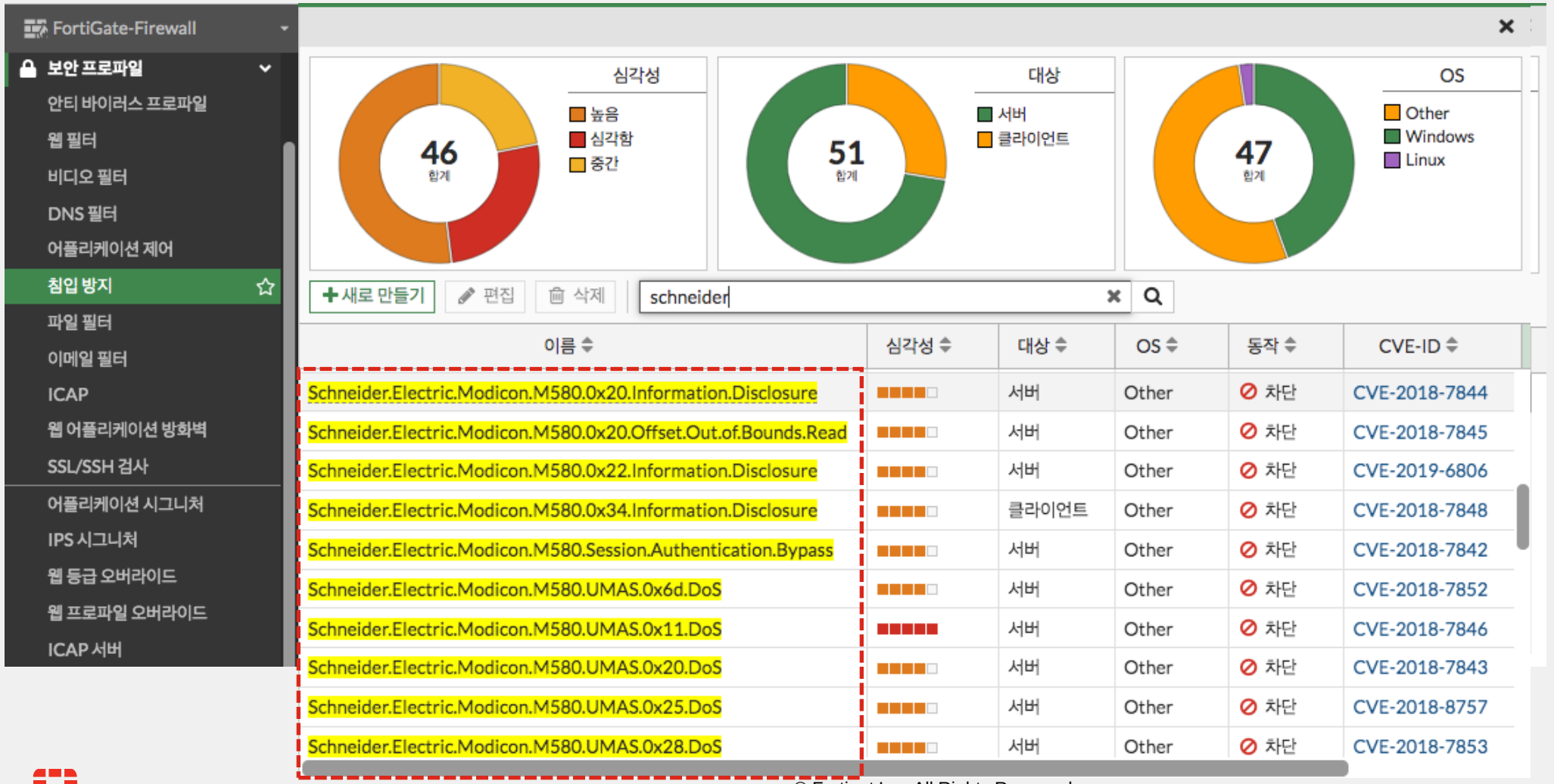
ICS-CVE (IPS)

보안 취약점이 발견된 OT 제조사 장비

- 7 Technologies / Schneider Electric
- ABB
- Advantech
- Broadwin
- CitectSCADA
- CoDeSys
- Cogent
- DATAC
- Eaton
- GE
- Iconics
- InduSoft
- IntelliCom
- Measuresoft
- Microsys
- MOXA
- PcVue
- Progea
- QNX
- RealFlex
- Rockwell Automation
- RSLogix
- Siemens
- Sunway
- TeeChart
- VxWorks
- WellinTech
- Yokogawa

2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

3)네트워크 트래픽 통제 : FortiGate NGFW(UTM)



2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

3)네트워크 트래픽 통제 : FortiGate NGFW(UTM)

```
(base) PS C:¥Users¥fortinet¥Downloads> python .¥modbus_read_registers.py
Starting register reads
Pump and conveyor are running
Pump and conveyor are running
Pump and conveyor are running
Pump and conveyor are running
Pump and conveyor are running
Pump and conveyor are running
Pump and conveyor are running
Pump and conveyor are running
Pump and conveyor are running
Pump and conveyor are running
Pump and conveyor are running
Pump and conveyor are running
Pump and conveyor are running
Pump and conveyor are running
Pump and conveyor are running
Pump and conveyor are running
```

컨베어벨트 정상 동작

FortiGateRugged 90D FGR90DT618000045

Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
User & Device
WiFi & Switch Controller
Log & Report
Forward Traffic
Local Traffic
Sniffer Traffic
Events
AntiVirus
Web Filter
SSL
DNS Query
Application Control

Add Filter | Details

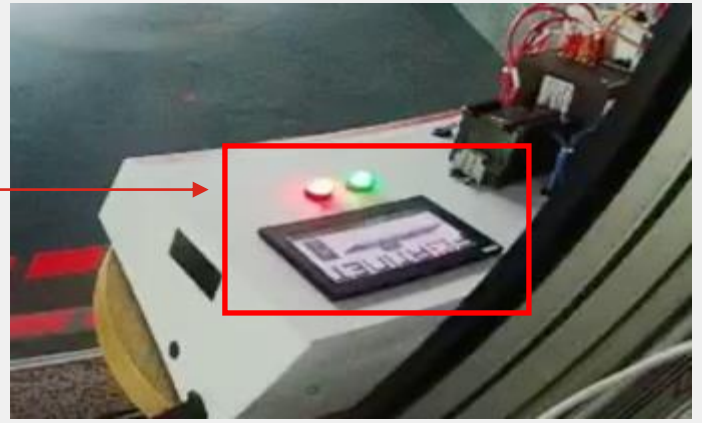
Date/Time	Source	Destination	Application Name	Action	Application User	Application Details
2020/10/17 11:41:16	192.168.14.13	192.168.1.4	Modbus_Read.Holding.Registers	pass		Read Holding Registers
2020/10/17 11:41:16	192.168.14.13	192.168.1.4	Modbus_Read.Holding.Registers	pass	192.168.14.13	Read Holding Registers: 00 00 00 02
2020/10/17 11:41:16	192.168.14.13	192.168.1.4	Modbus_Read.Holding.Registers	pass	192.168.1.4	Read Holding Registers: 04 00 00 00 01
2020/10/17 11:41:16	192.168.14.13	192.168.1.4	Modbus_Read.Holding.Registers	pass		Read Holding Registers
2020/10/17 11:41:16	192.168.14.13	192.168.1.4	Modbus_Read.Holding.Registers	pass	192.168.14.13	Read Holding Registers: 00 00 00 02
2020/10/17 11:41:14	192.168.14.13	192.168.1.4	Modbus_Read.Holding.Registers	pass	192.168.1.4	Read Holding Registers: 04 00 00 00 01
2020/10/17 11:41:14	192.168.14.13	192.168.1.4	Modbus_Read.Holding.Registers	pass		Read Holding Registers
2020/10/17 11:41:14	192.168.14.13	192.168.1.4	Modbus_Read.Holding.Registers	pass	192.168.14.13	Read Holding Registers: 00 00 00 02
2020/10/17 11:41:14	192.168.14.13	192.168.1.4	Modbus_Read.Holding.Registers	pass	192.168.1.4	Read Holding Registers: 04 00 00 00 01
2020/10/17 11:41:14	192.168.14.13	192.168.1.4	Modbus_Read.Holding.Registers	pass		Read Holding Registers
2020/10/17 11:41:14	192.168.14.13	192.168.1.4	Modbus_Read.Holding.Registers	pass	192.168.14.13	Read Holding Registers: 00 00 00 02
2020/10/17 11:41:12	192.168.14.13	192.168.1.4	Modbus_Read.Holding.Registers	pass	192.168.1.4	Read Holding Registers: 04 00 00 00 01
2020/10/17 11:41:12	192.168.14.13	192.168.1.4	Modbus_Read.Holding.Registers	pass		Read Holding Registers
2020/10/17 11:41:12	192.168.14.13	192.168.1.4	Modbus_Read.Holding.Registers	pass	192.168.14.13	Read Holding Registers: 00 00 00 02
2020/10/17 11:41:12	192.168.14.13	192.168.1.4	Modbus_Read.Holding.Registers	pass	192.168.1.4	Read Holding Registers: 04 00 00 00 01
2020/10/17 11:41:12	192.168.14.13	192.168.1.4	Modbus_Read.Holding.Registers	pass		Read Holding Registers

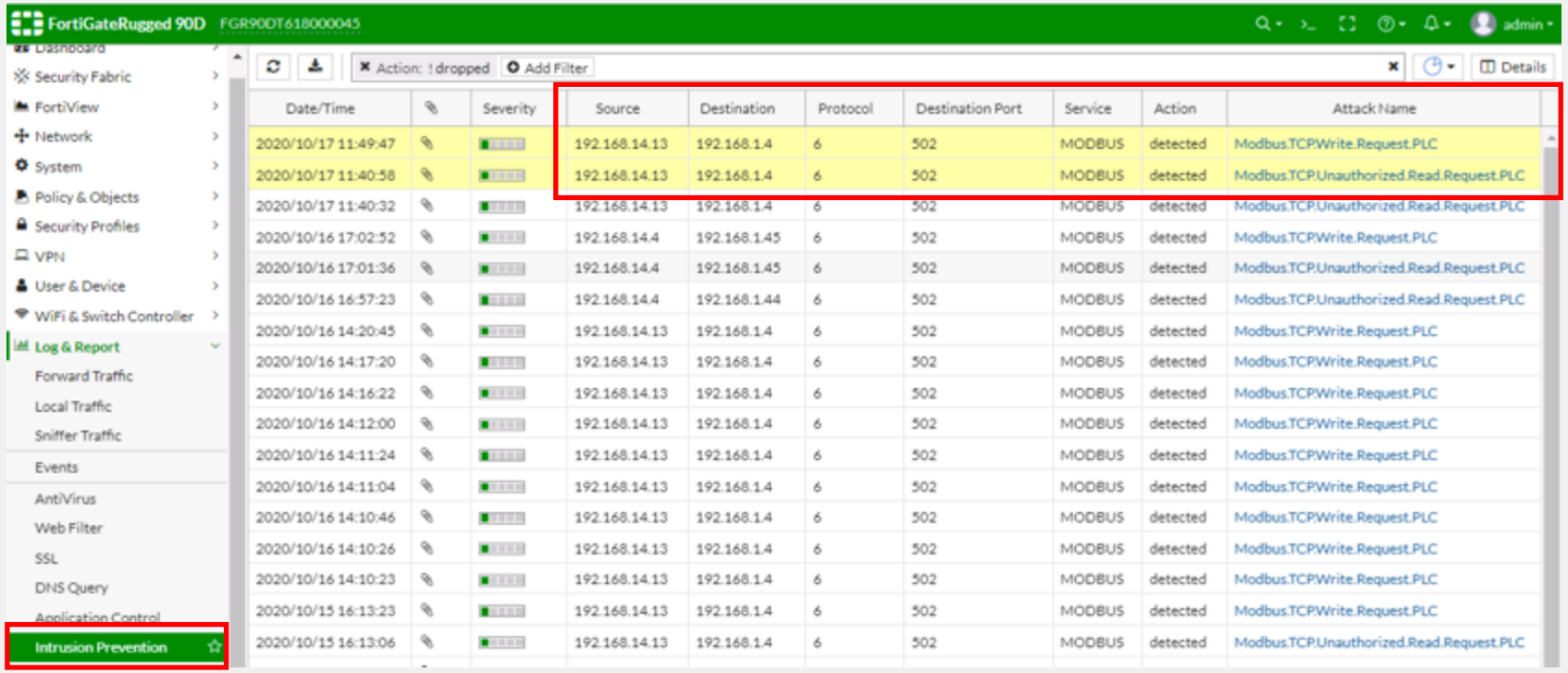
2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

3)네트워크 트래픽 통제 : FortiGate NGFW(UTM)

```
(base) PS C:₩Users₩fortinet₩Downloads> python .₩modbus_attack_random.py
(base) PS C:₩Users₩fortinet₩Downloads>
>>
>>
>>
>>
>>
>>
```

컨베어벨트 비 정상 동작

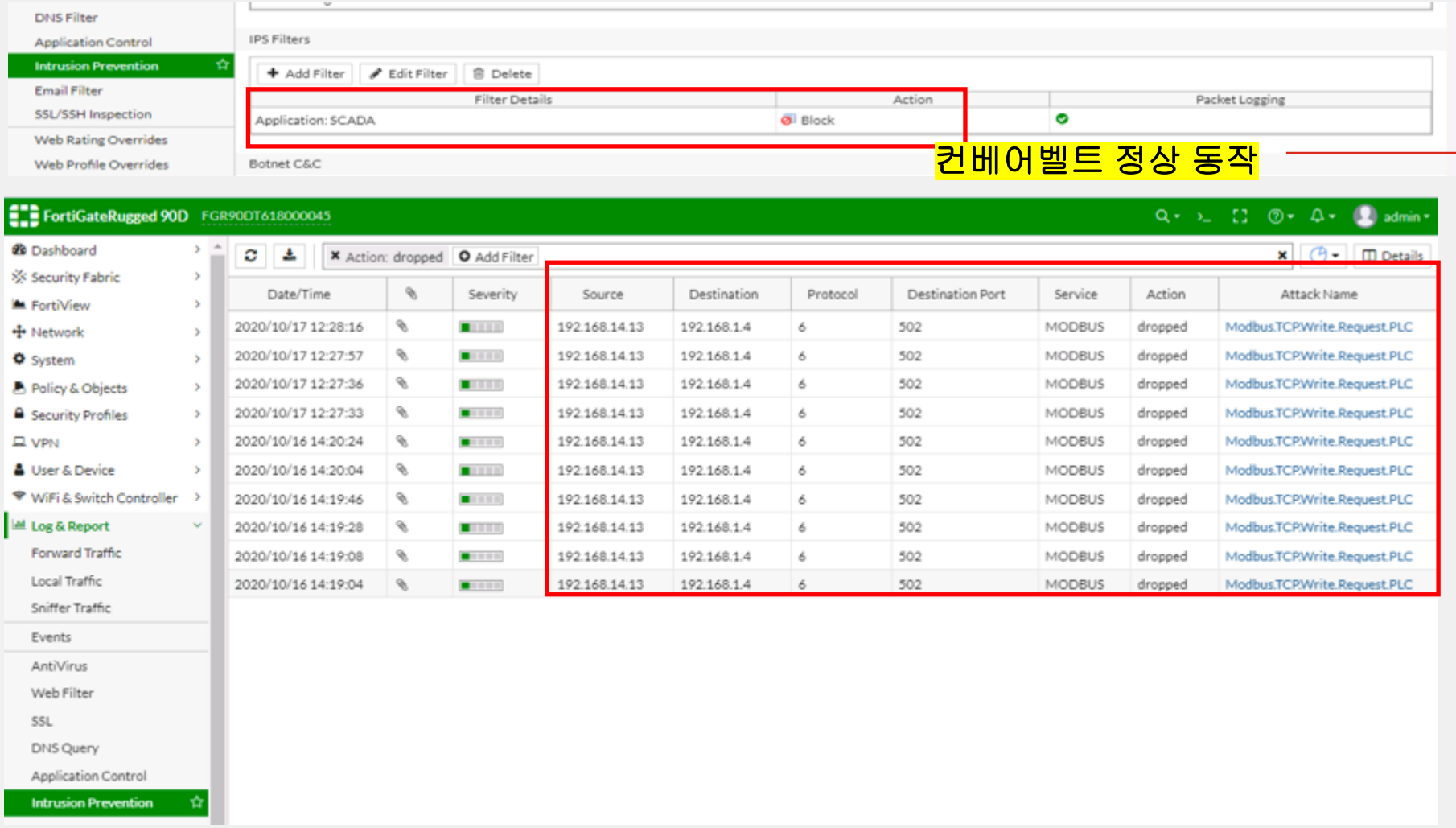




Date/Time	Severity	Source	Destination	Protocol	Destination Port	Service	Action	Attack Name
2020/10/17 11:49:47		192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCP.Write.Request.PLC
2020/10/17 11:40:58		192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCP.Unauthorized.Read.Request.PLC
2020/10/17 11:40:32		192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCP.Unauthorized.Read.Request.PLC
2020/10/16 17:02:52		192.168.14.4	192.168.1.45	6	502	MODBUS	detected	Modbus.TCP.Write.Request.PLC
2020/10/16 17:01:36		192.168.14.4	192.168.1.45	6	502	MODBUS	detected	Modbus.TCP.Unauthorized.Read.Request.PLC
2020/10/16 16:57:23		192.168.14.4	192.168.1.44	6	502	MODBUS	detected	Modbus.TCP.Unauthorized.Read.Request.PLC
2020/10/16 14:20:45		192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCP.Write.Request.PLC
2020/10/16 14:17:20		192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCP.Write.Request.PLC
2020/10/16 14:16:22		192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCP.Write.Request.PLC
2020/10/16 14:12:00		192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCP.Write.Request.PLC
2020/10/16 14:11:24		192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCP.Write.Request.PLC
2020/10/16 14:11:04		192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCP.Write.Request.PLC
2020/10/16 14:10:46		192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCP.Write.Request.PLC
2020/10/16 14:10:26		192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCP.Write.Request.PLC
2020/10/16 14:10:23		192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCP.Write.Request.PLC
2020/10/15 16:13:23		192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCP.Write.Request.PLC
2020/10/15 16:13:06		192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCP.Unauthorized.Read.Request.PLC

2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

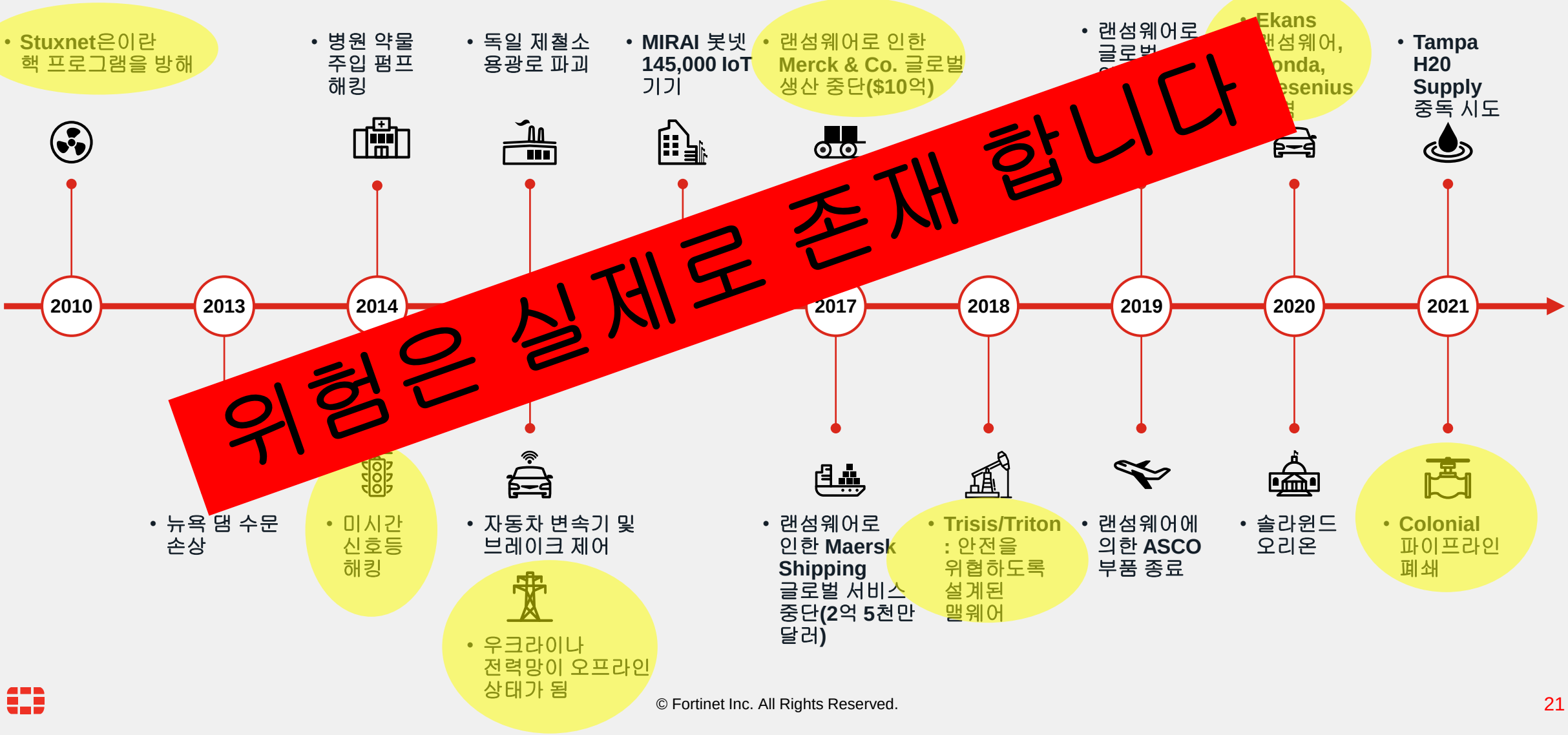
3)네트워크 트래픽 통제 : FortiGate NGFW(UTM)



컨베어벨트 정상 동작

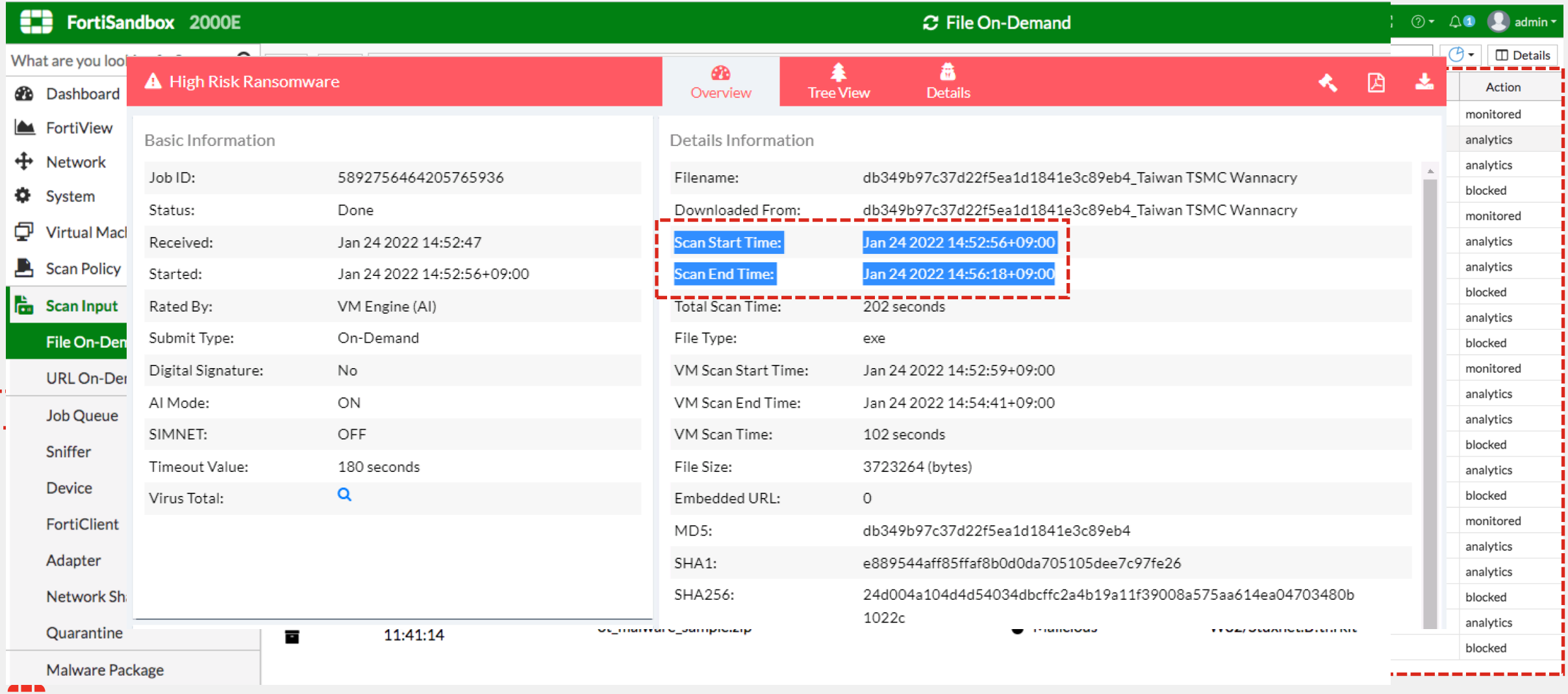
3. 랜섬웨어 및 악성코드 탐지/차단 솔루션

- FortiSandbox / FortiAI / FortiEDR



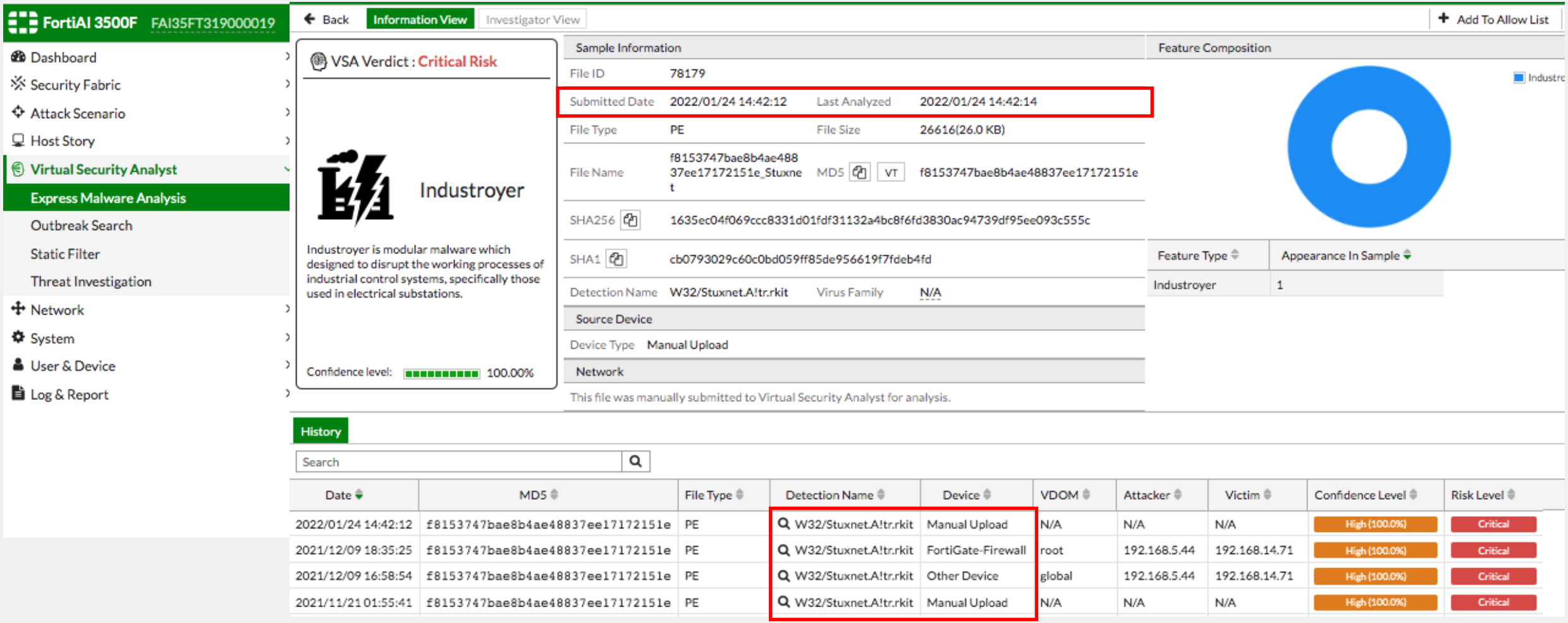
3. 랜섬웨어 및 악성코드 탐지/차단 솔루션

- FortiSandbox / FortiAI / FortiEDR



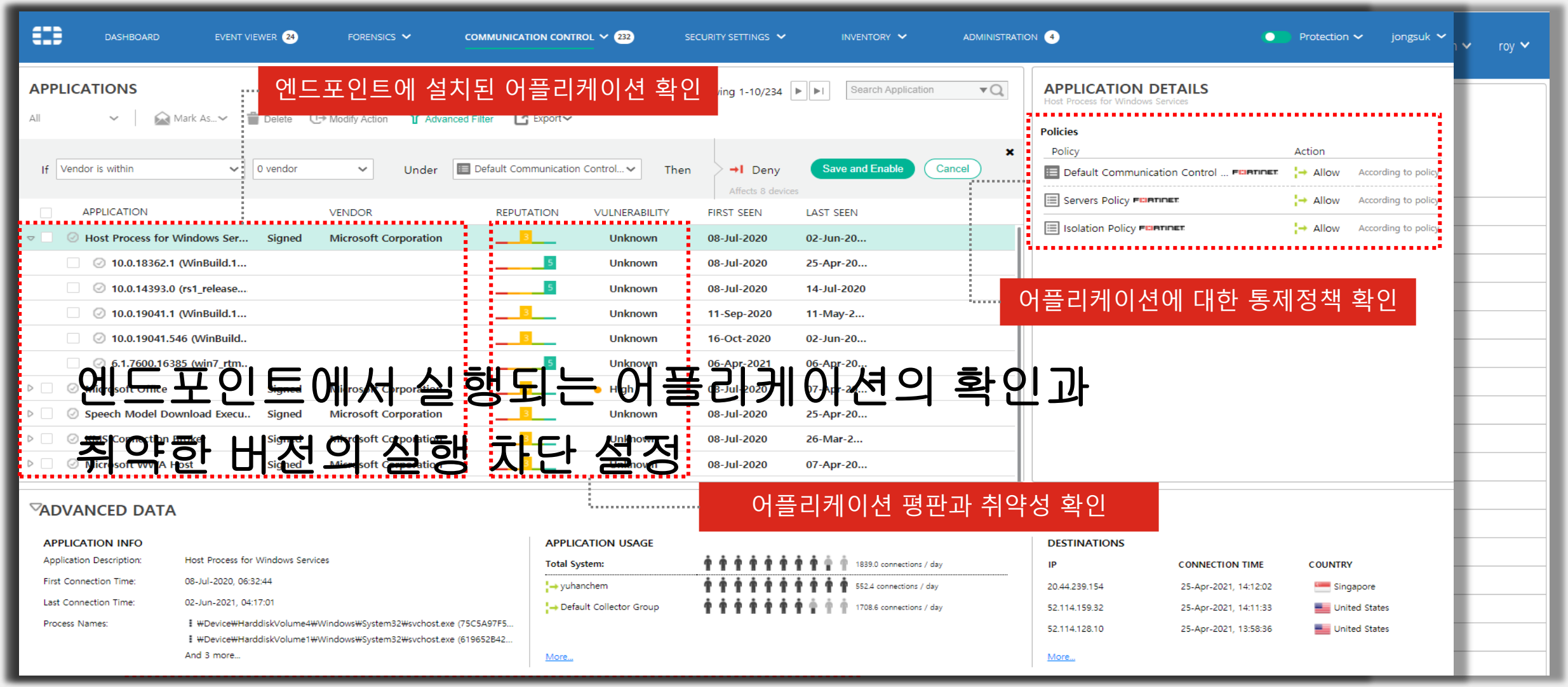
3. 랜섬웨어 및 악성코드 탐지/차단 솔루션

- FortiSandbox / FortiAI / FortiEDR



3. 랜섬웨어 및 악성코드 탐지/차단 솔루션

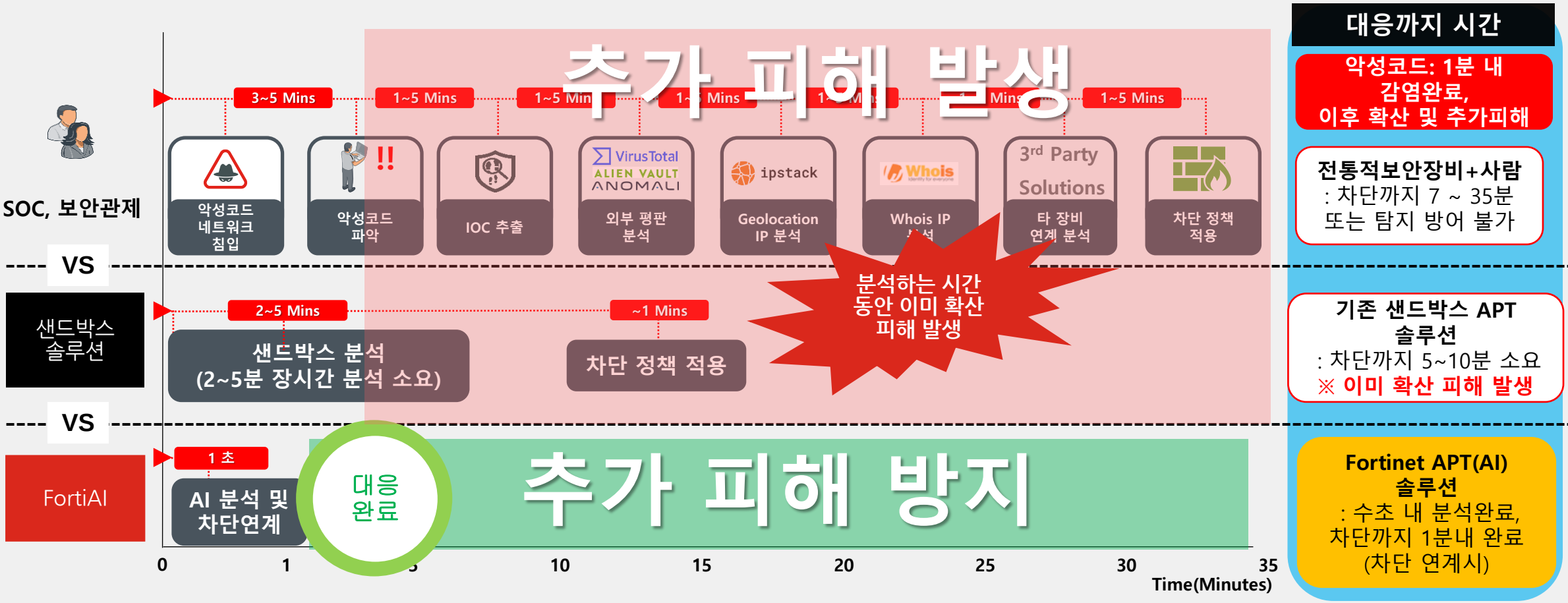
- FortiSandbox / FortiAI / FortiEDR



3. 랜섬웨어 및 악성코드 탐지/차단 솔루션

- FortiSandbox / FortiAI / FortiEDR

▪ 기존 ATP 시스템의 느린 대응점 해소



4. 안전한 VPN 접속 및 VPN 통신의 효율성 극대화 솔루션

- SSL VPN with FortiClientEMS

시나리오1. 제조/공장망 접속 단말이 특정 OS 및 Anti-Virus 설치가 가능 할 때 접속 허용

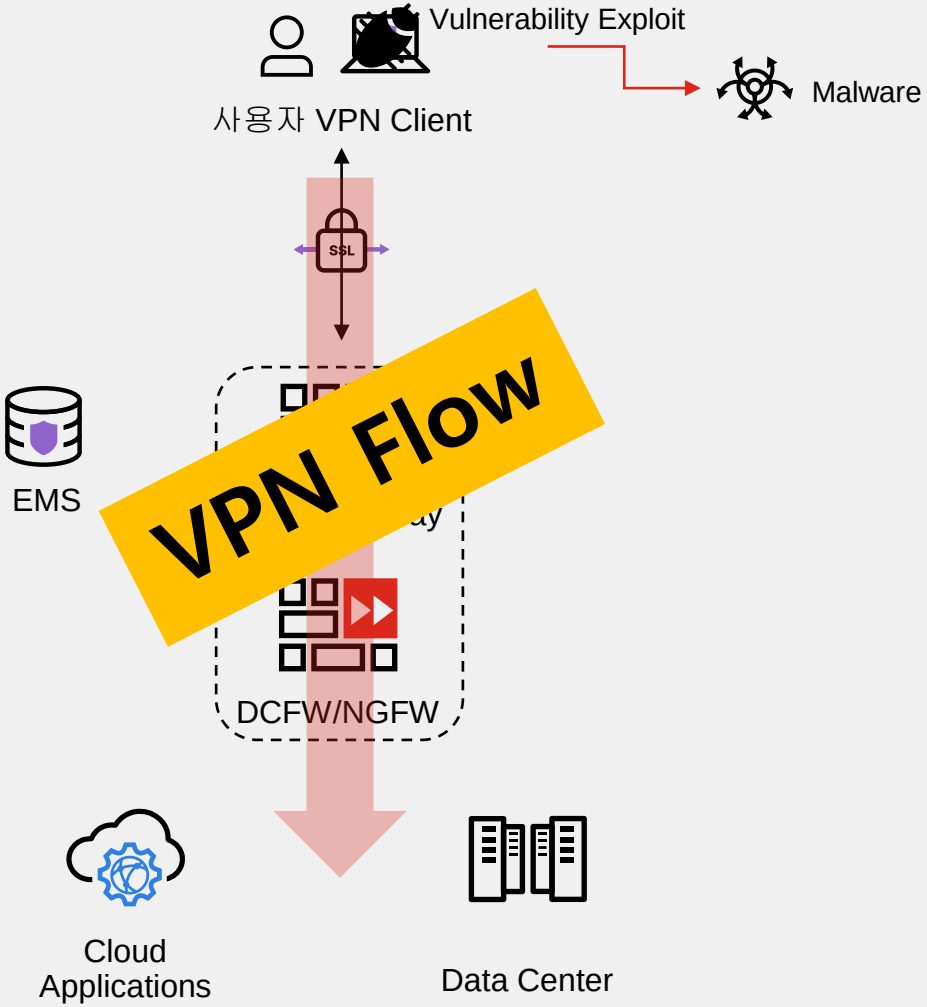
- 제로트러스트(ZTNA) 태그 룰
  - Windows 10
  - Anti-Virus 설치

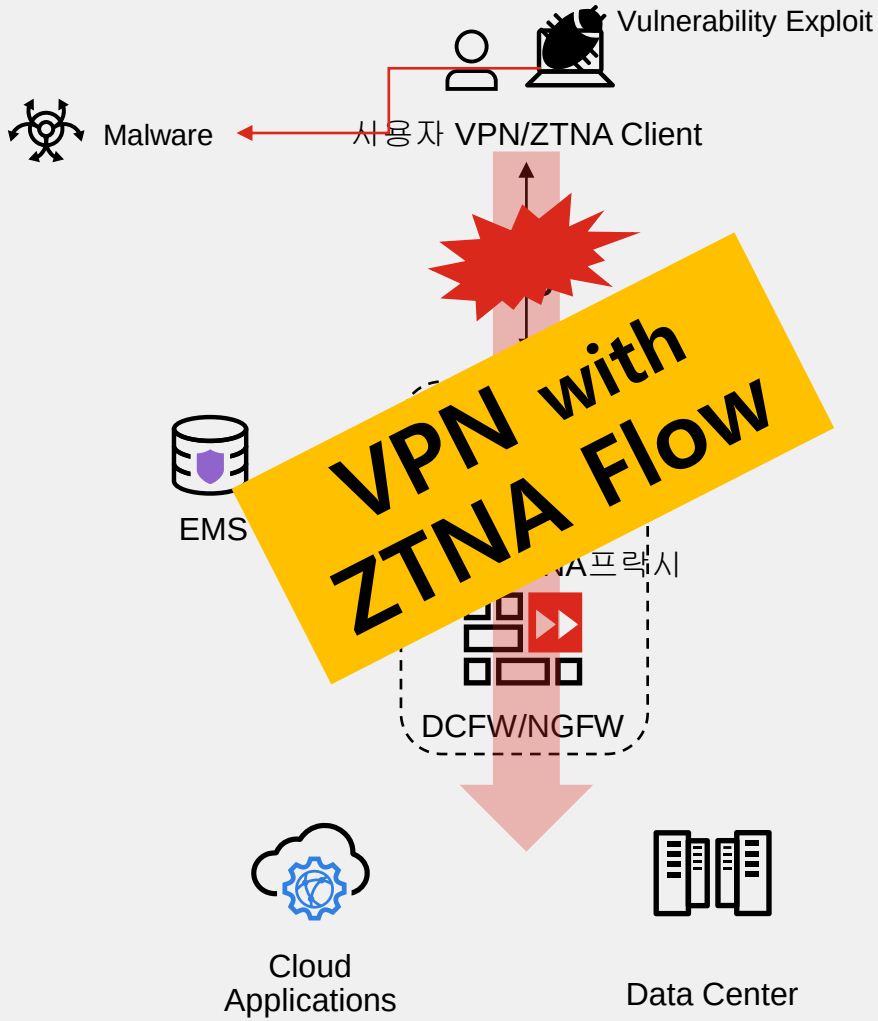
시나리오2. 제조/공장망 접속 단말이 old OS, Anti-Virus 미 설치, 악성코드에 감염된 경우 즉각 차단

- 제로트러스트(ZTNA) 태그 룰
  - Windows 7
  - Anti-Virus 미 설치
  - ATP(FortiSandbox) 탐지 내역

4. 안전한 VPN 접속 및 VPN 통신의 효율성 극대화 솔루션

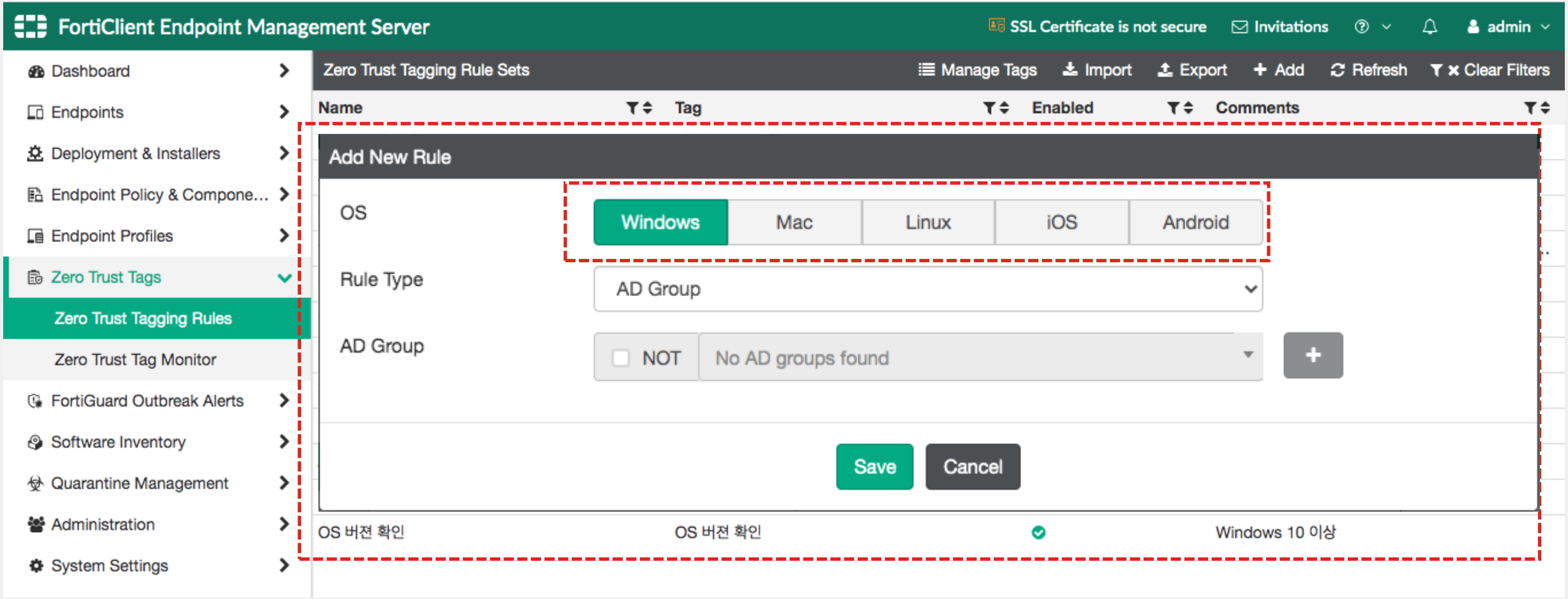
- SSL VPN with FortiClientEMS





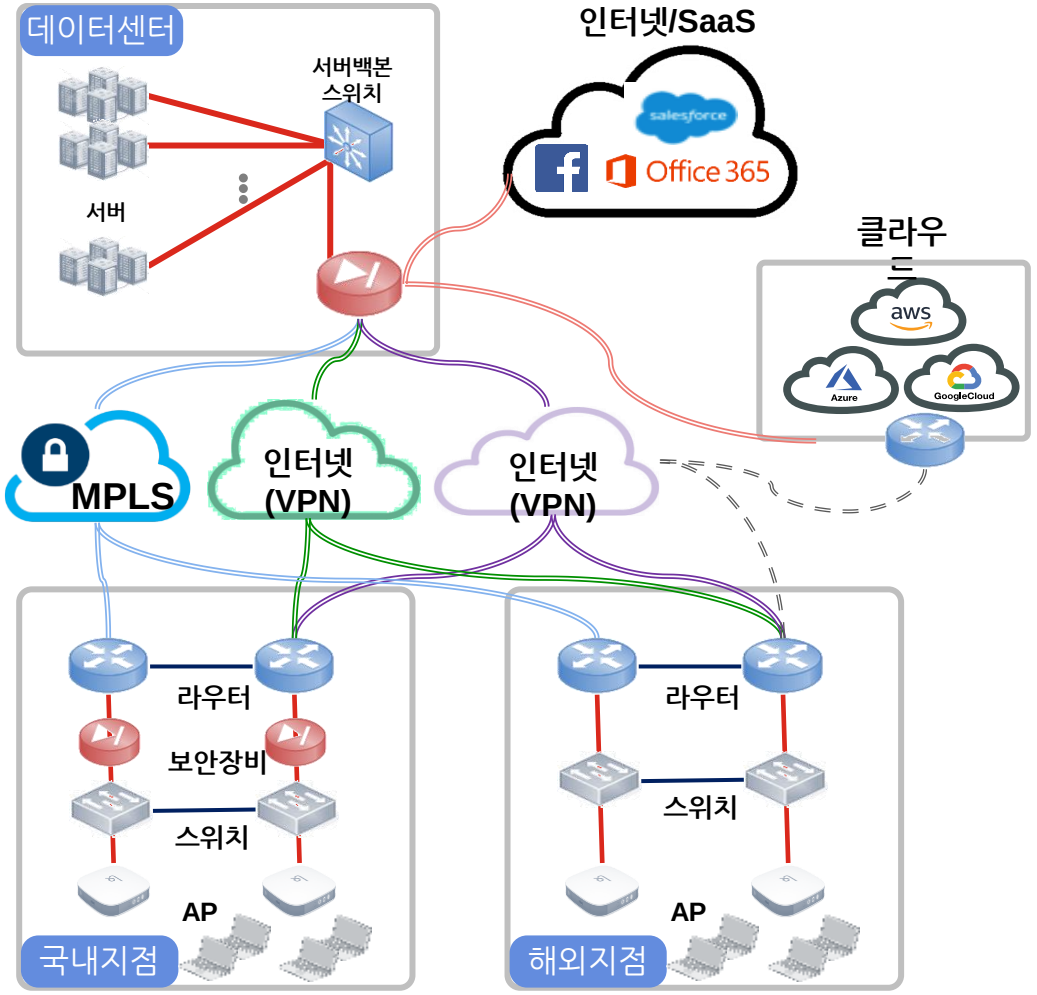
4. 안전한 VPN 접속 및 VPN 통신의 효율성 극대화 솔루션

- SSL VPN with FortiClientEMS



4. 안전한 VPN 접속 및 VPN 통신의 효율성 극대화 솔루션

- FortiGate SD-WAN



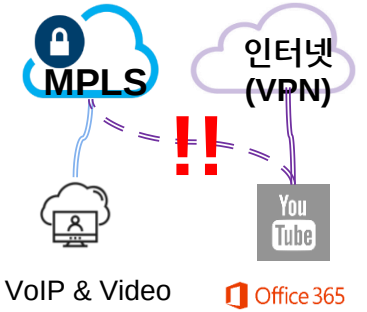
트래픽 가시성

네트워크상의 트래픽에 대한 가시성 부족

회선 대역폭의 효율적인 사용

모든 트래픽을 데이터센터의 보안 장비를 거쳐 통신, 어플리케이션별 라우팅 불가

대용량 트래픽의 MPLS 회선 사용



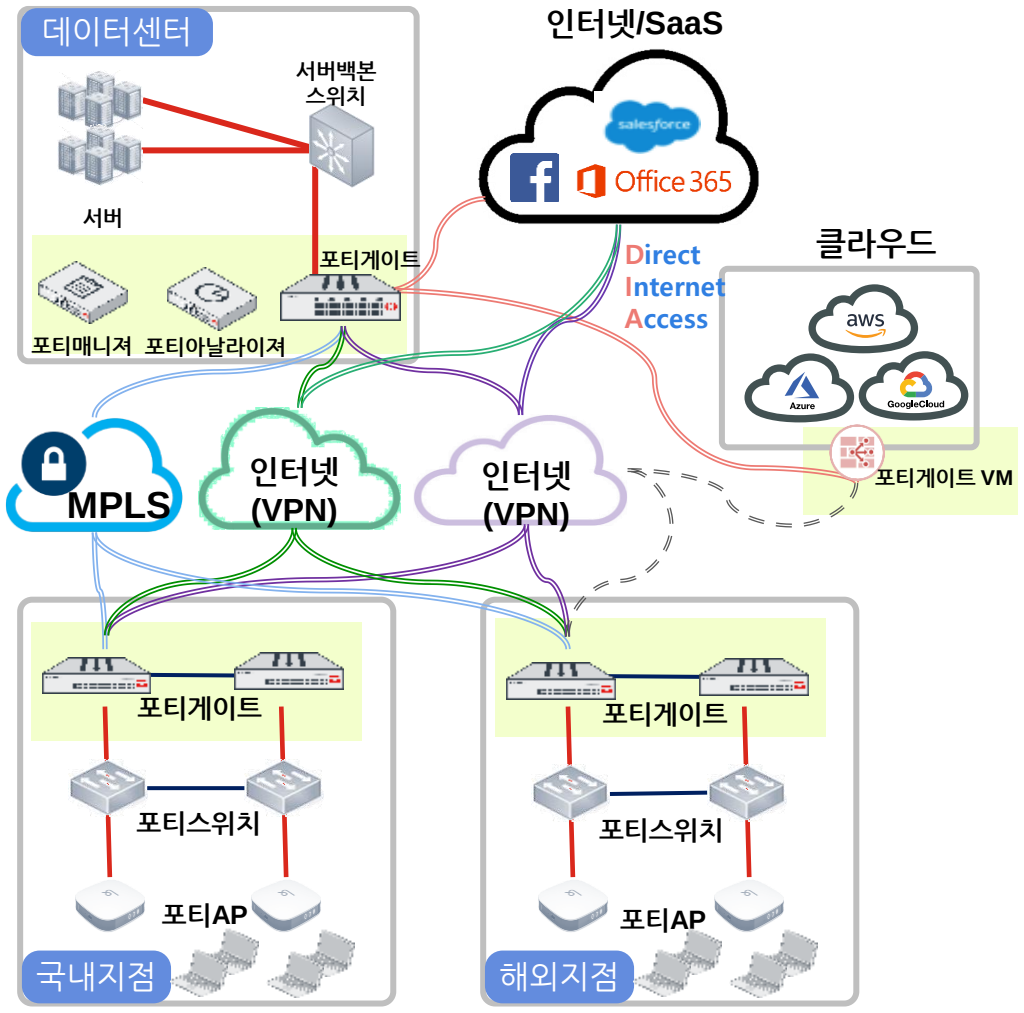
Cloud 및 SaaS 접속

Direct Cloud Access로 사용자 만족도 개선

해외 지점은 해당 리전 SaaS 사용으로 사용자 만족도 향상

4. 안전한 VPN 접속 및 VPN 통신의 효율성 극대화 솔루션

- FortiGate SD-WAN



트래픽 가시성

트래픽에 대한 가시성 확보

포티아날라이저를 통해

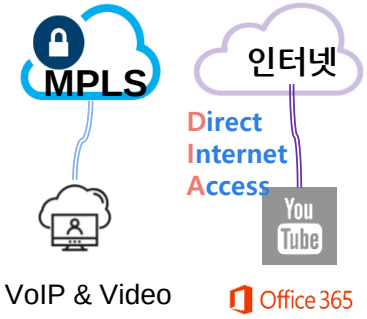
전 지점 트래픽 통합 모니터링

회선 대역폭의 효율적인 사용

비업무 트래픽 Direct Internet Access

Application별 라우팅 적용

대용량 대역폭 사용 트래픽에 대한 제어



Cloud 및 SaaS 접속

Direct Cloud Access로 사용자 만족도 개선

해외 지점은 해당 리전 SaaS 사용으로

사용자 만족도 향상

4. 안전한 VPN 접속 및 VPN 통신의 효율성 극대화 솔루션

- FortiGate SD-WAN

순서	용도	Application	Preferred WAN Link	SD-WAN rule
1	기업 내부 DC 접속	Internal IP address	VPN_1 VPN_2 **Overlay(오버레이)**	Lowest Cost
2	Voice & Video	Internal IP address	VPN_1 VPN_2	Lowest Cost or Best Quality (Lab)
3	Business Critical 인터넷	Salesforce Microsoft O365	VPN_2 ISP_1 **Underlay/Overlay**	Lowest Cost
4	Business Non-critical 인터넷	Microsoft Update	ISP_2 VPN_1	Lowest Cost (Lab) or Maximize BW
5	Non_business 인터넷	Other 인터넷	ISP_2 **Underlay(언더레이)**	Manual
6	Implicit	Implicit	All	N/A

결론

1. 제조환경/ 공장에서 발생 가능한 보안 이슈

2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

   1)네트워크 인프라 가시성 확보 : FortiGate / FortiSwitch / FortiAP

   2) 공장망 망분리 세분화 : FortiGate / FortiSwitch

   3) 네트워크 트래픽 통제 : FortiGate NGFW(UTM)

3. 랜섬웨어 및 악성코드 탐지/차단 솔루션

   - FortiSandbox / FortiAI / FortiEDR

4. 안전한 VPN 접속 및 VPN 통신의 효율성 극대화 솔루션

   - SSL VPN with FortiClientEMS, FortiGate SD-WAN


FORTINET