



제조업 고객사를 위한 포티넷 보안 솔루션 소개 웨비나

포티넷 코리아 SE팀 / 김기환

Q1, 2022

목차

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



1. 제조환경/ 공장에서 발생 가능한 보안 이슈



1. 제조환경/ 공장에서 발생 가능한 보안 이슈



동영상 별도 Play

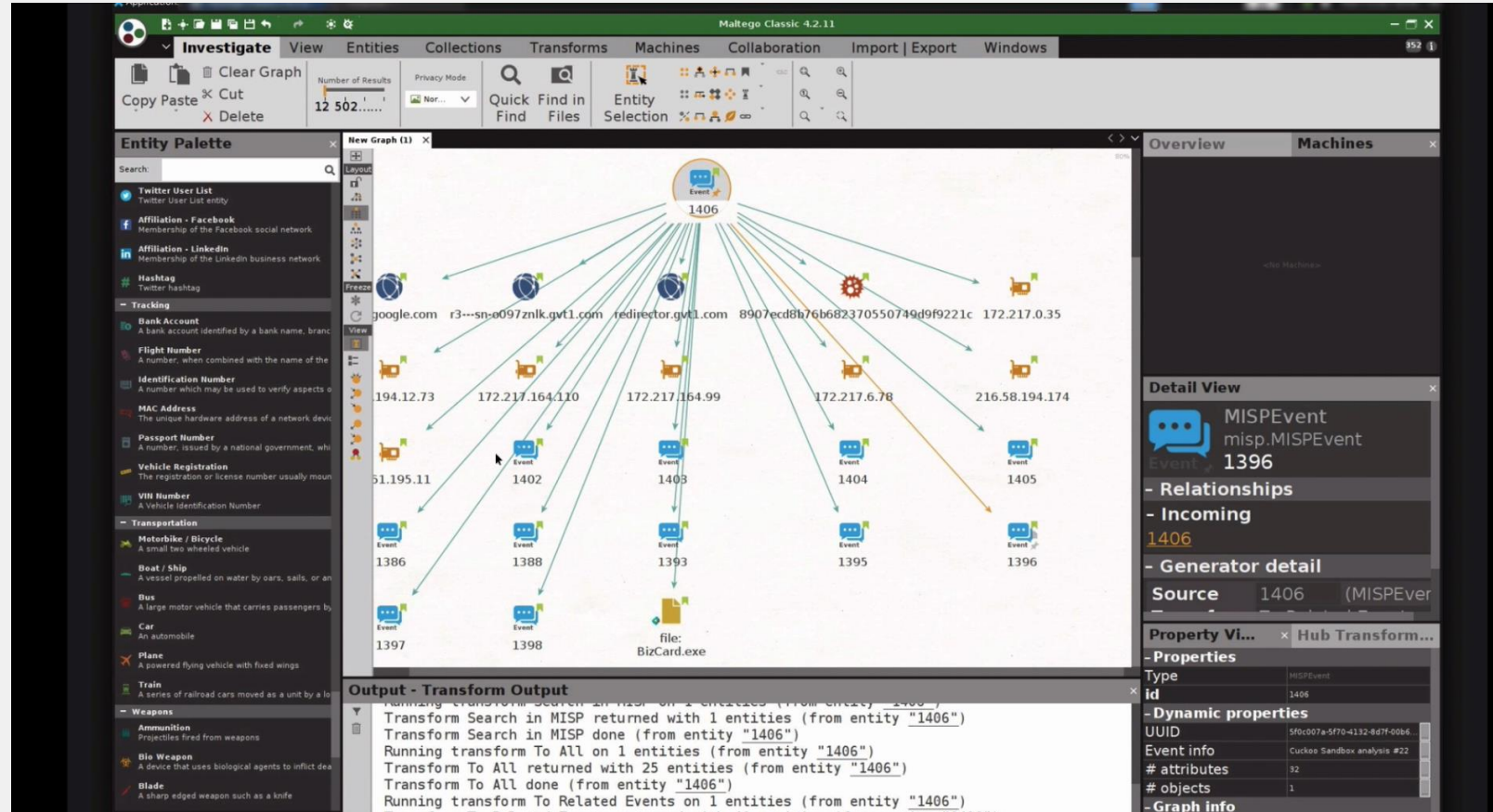


1. 제조환경/ 공장에서 발생 가능한 보안 이슈



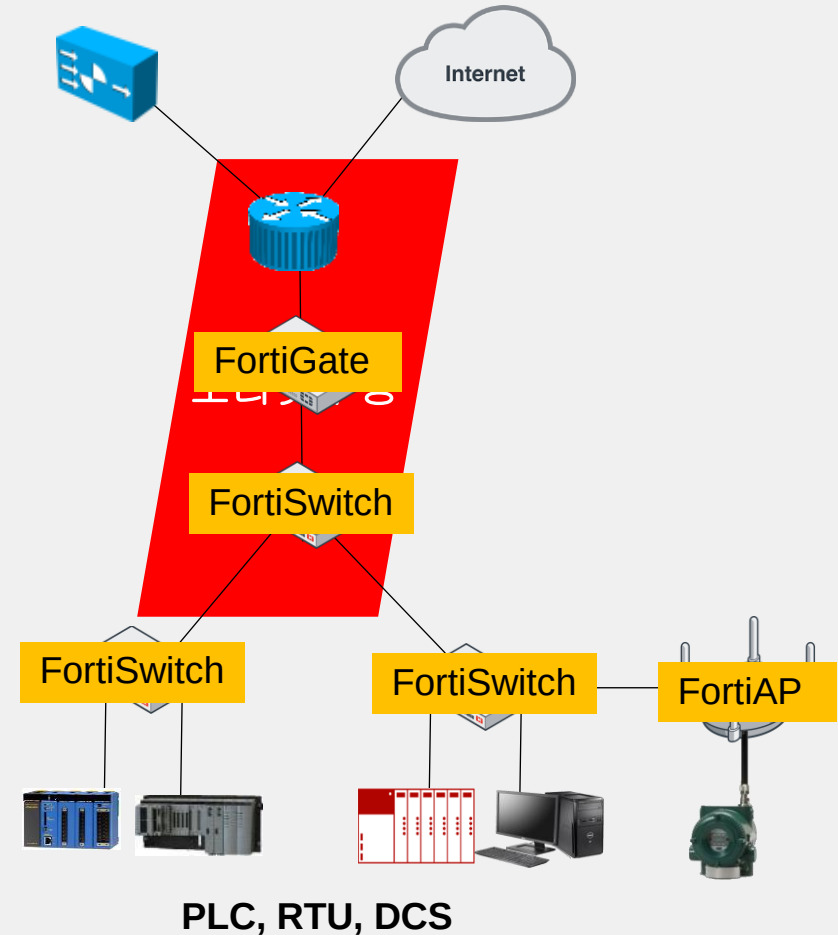
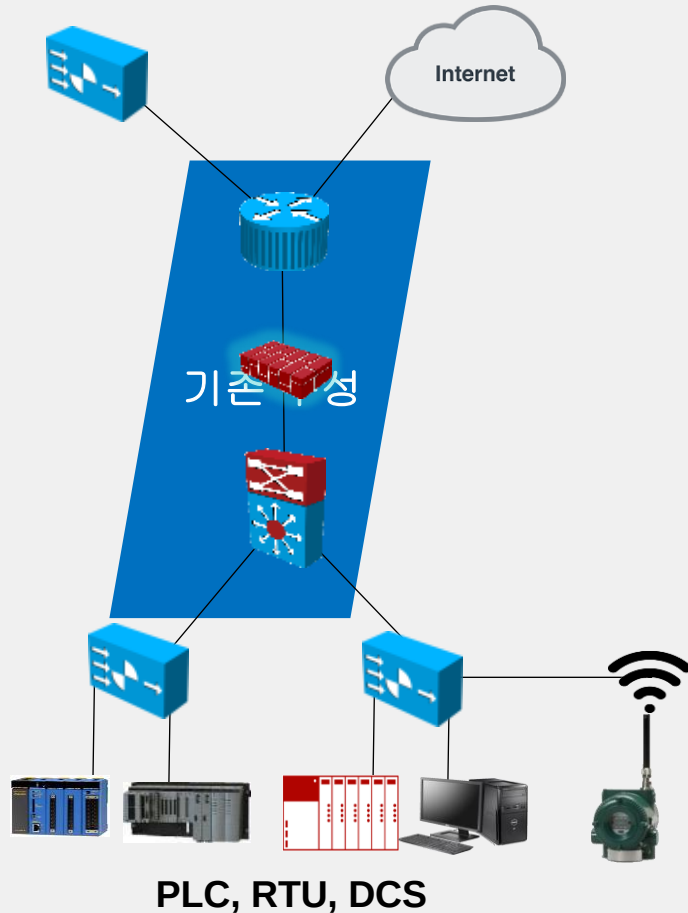
동영상 별도 Play

1. 제조환경/ 공장에서 발생 가능한 보안 이슈



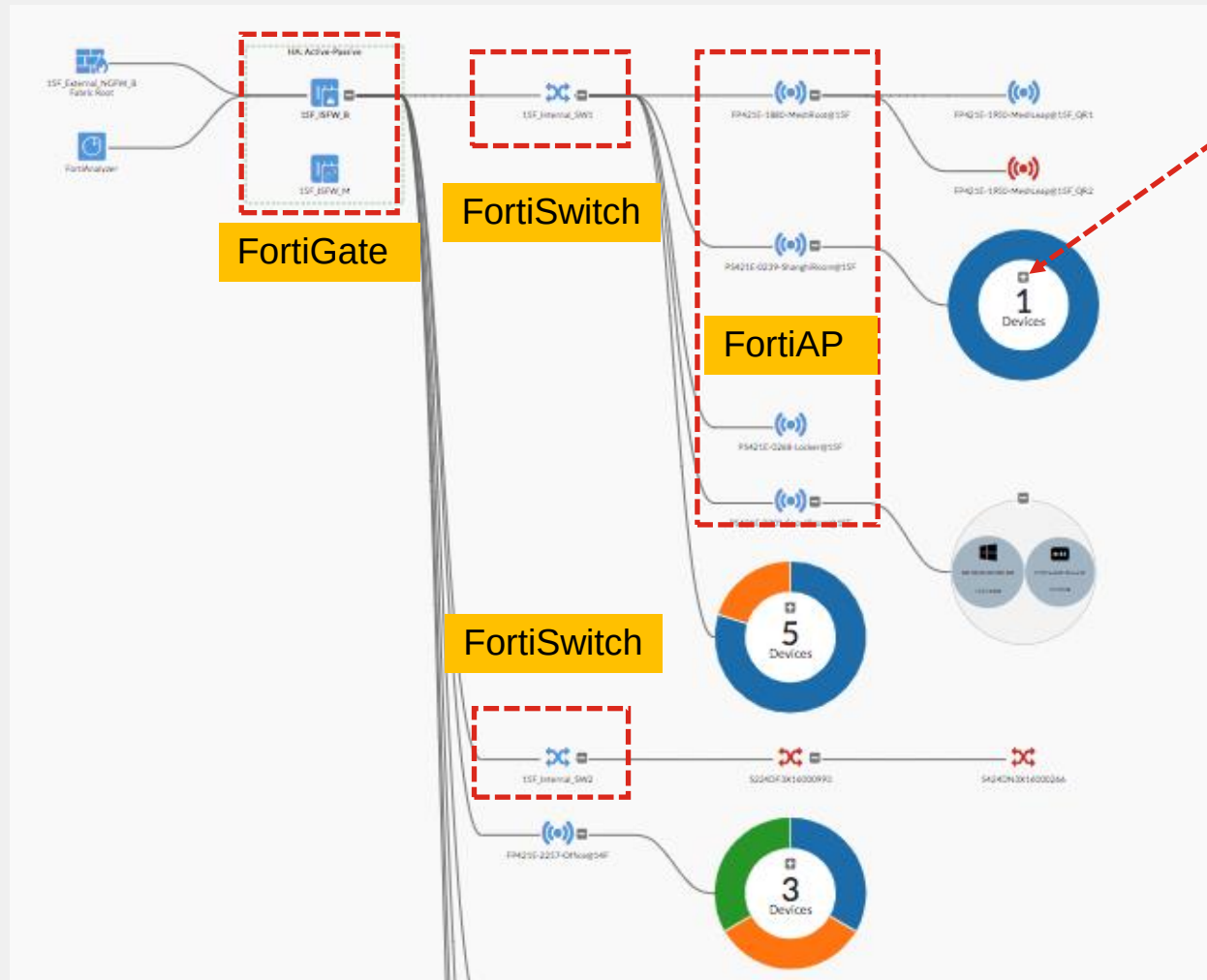
2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

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



2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

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



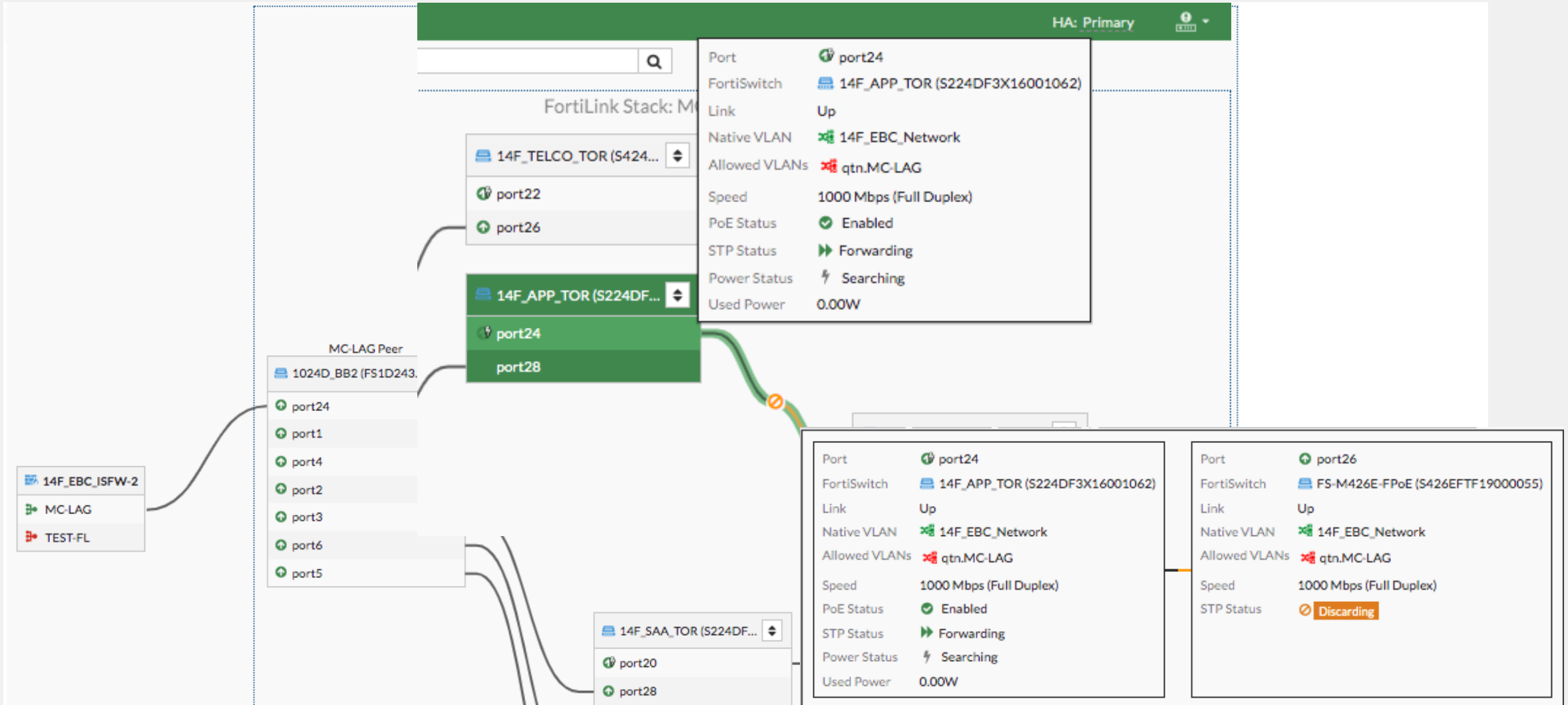
192.168.1.51

Device	WINDOWS-S2ECD7M
MAC Address	00:01:23:42:4e:83
IP Address	192.168.1.51
Online Interfaces	OT VLAN (S524DN4K17000110:port3)
Hardware	Schneider Elect / Energy
OS	Windows / 7
Detected By	FortiGuard IoT detection service
Topology	FortiGate-Firewall S524DN4K17000110 WINDOWS-S2ECD7M
Sessions	1
Bytes (Sent/Received)	3.74 GB
Bandwidth	78.37 kbps
Packets (Sent/Received)	48.86 MB

+ Firewall Device Address + Firewall IP Address Quarantine Host

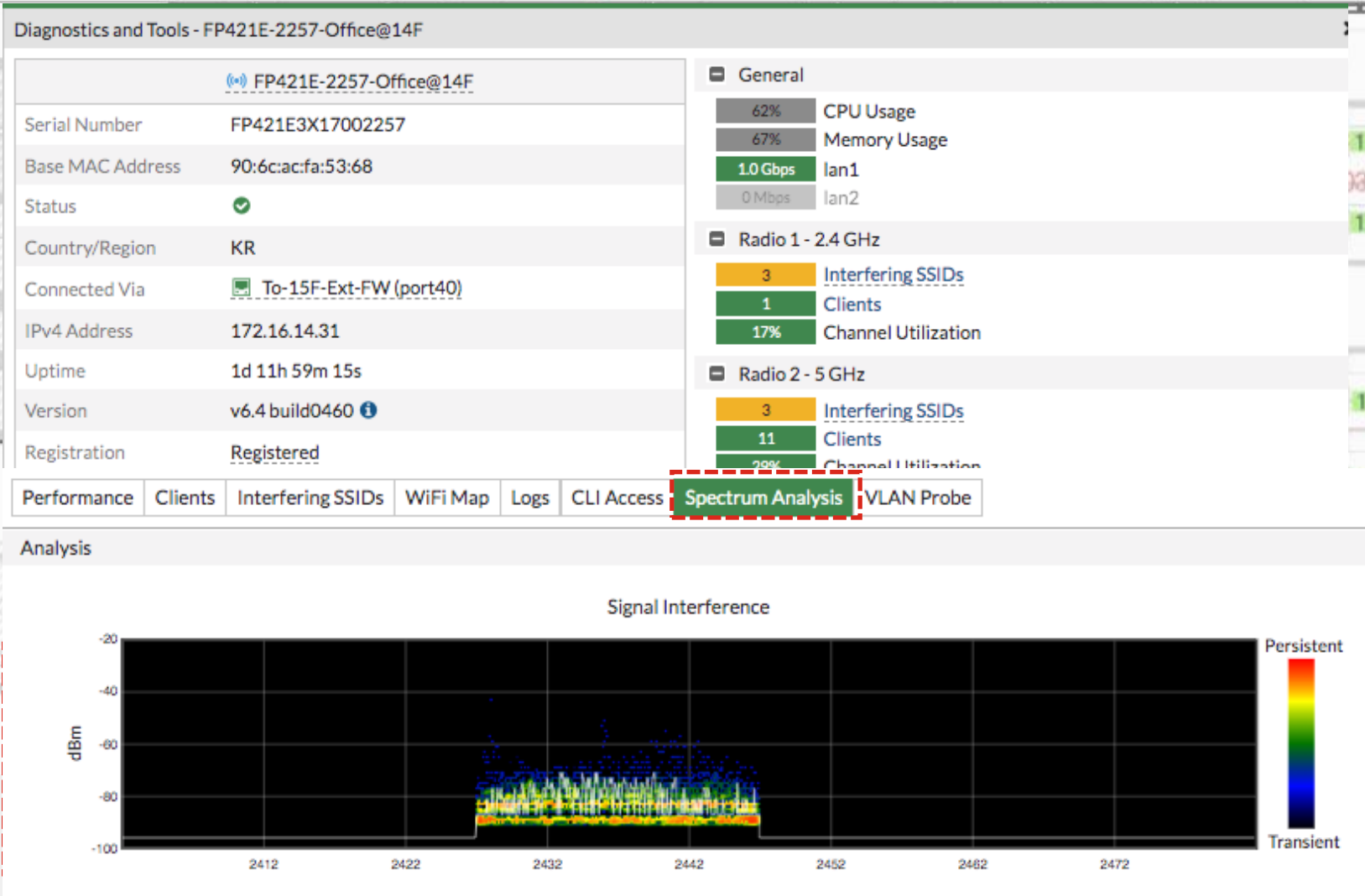
2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

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



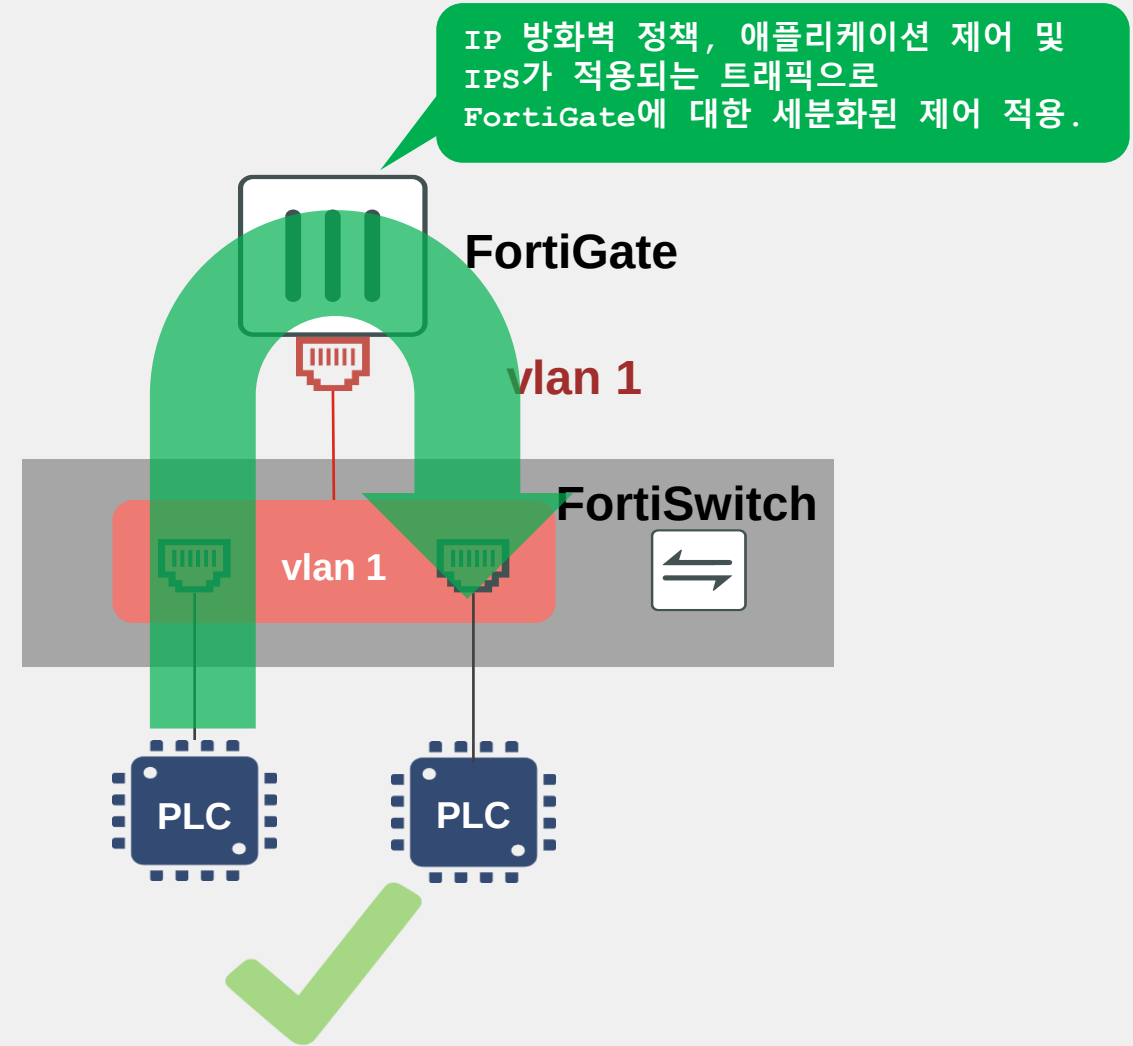
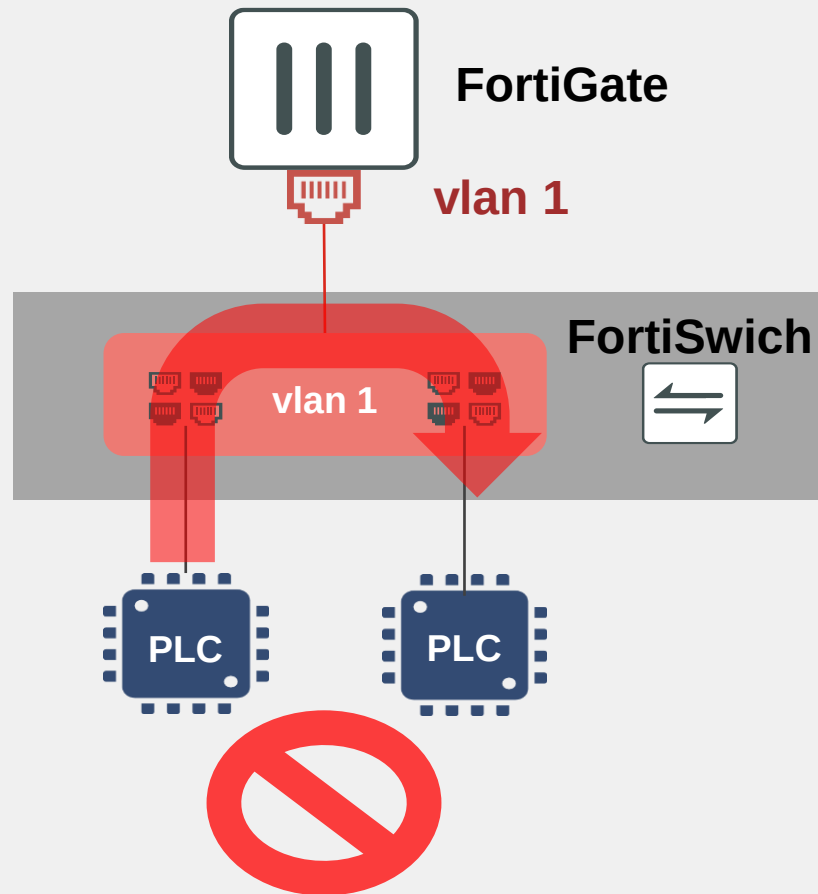
2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

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



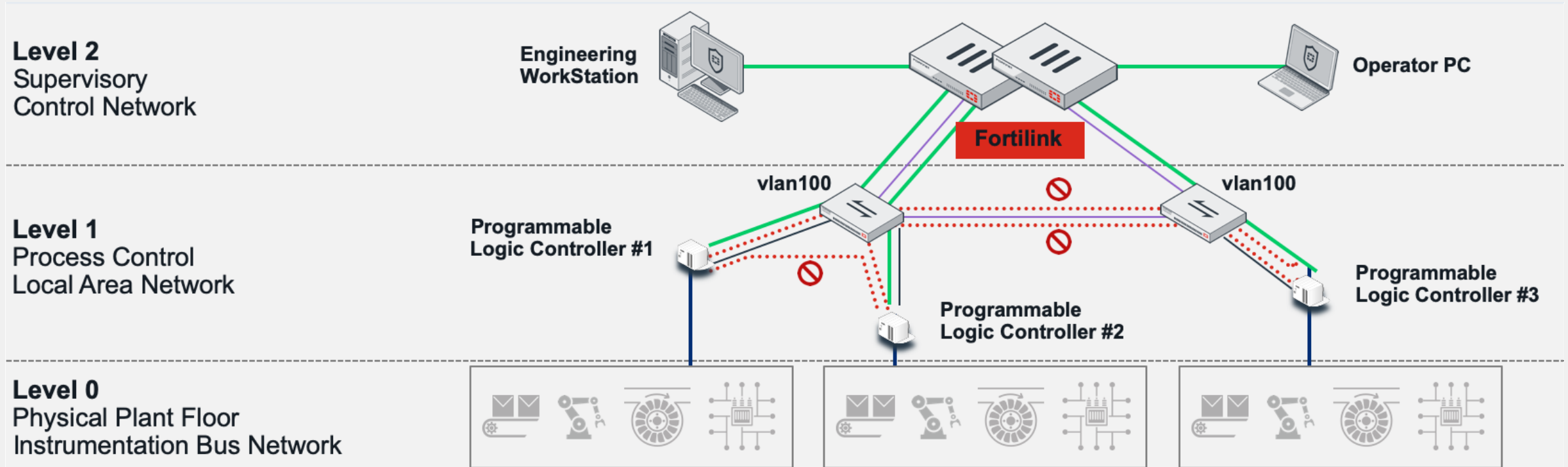
2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

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

FortiGate-Firewall

대시보드
네트워크
정책 및 객체
방화벽 정책
로컬 정책
IPv4 DoS 정책
프로시 정책
ZTNA
인증 규칙

이름
에서
목적지 인터페이스
출발지
목적지
서비스
보안 프로파일
바이트
현재 세션
패킷

OT-VLAN10_마이크로 세그먼트	OT-VLAN 10 (OT VLAN)	OT-VLAN 10 (OT VLAN)	Schneider_HMI_192.168.1.51	Schneider_PLC_192.168.1.31	OT_Modbus_TCP_502 ALL_ICMP	OT 어플리케이션 certificate-inspection	6.79 GB	3	88,794,309
IT zone to OT zone	IT Zone (wan1)	OT Zone (port2)	all	all	ALL	certificate-inspection	4.32 GB	158	48,039,408
OT Zone to IT Zone	OT Zone (port2)	IT Zone (wan1)	all	all	ALL	Demo1 Demo1 OT 어플리케이션 OT 침입방지 custom-deep-inspection	1.53 GB	11	4,431,850

FortiGate-Firewall

대시보드
네트워크
정책 및 객체
보안 프로파일
VPN
사용자 및 인증
WiFi 및 스위치 컨트롤러
시스템
시큐리티 패브릭
로그 및 보고서
포워드 트래픽

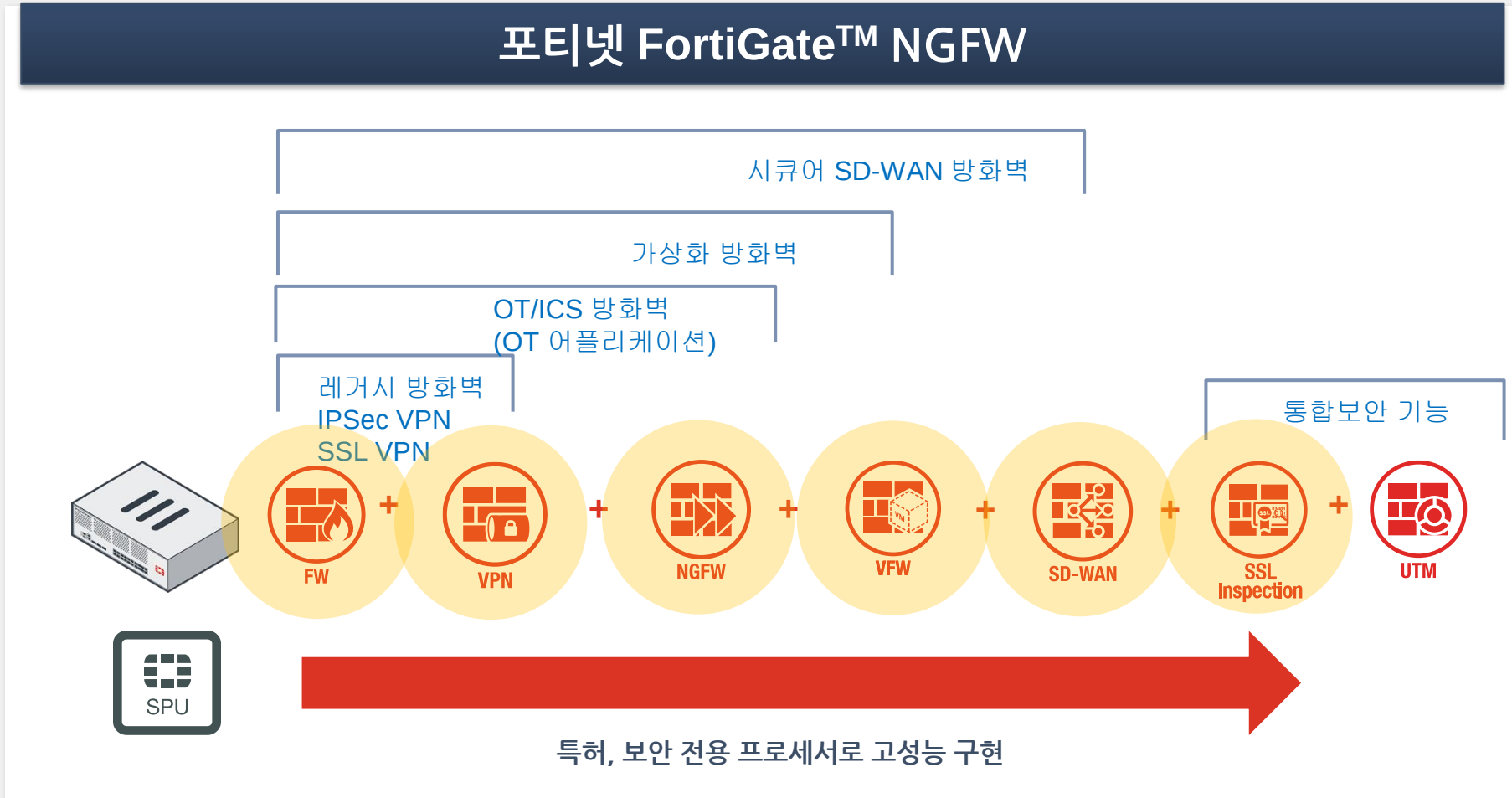
Absolute Date/Time
출발지 IP
목적지 IP
어플리케이션 이름
결과
정책

2022-01-24 01:17:19	192.168.1.51	192.168.1.31	Modbus_Read.Holding.Registers	✓ 1.29 GB / 2.51 GB	OT-VLAN10_마이크로 세그먼트 (13)
2022-01-24 01:15:19	192.168.1.51	192.168.1.31	Modbus_Read.Holding.Registers	✓ 1.29 GB / 2.51 GB	OT-VLAN10_마이크로 세그먼트 (13)
2022-01-24 01:13:19	192.168.1.51	192.168.1.31	Modbus_Read.Holding.Registers	✓ 1.29 GB / 2.51 GB	OT-VLAN10_마이크로 세그먼트 (13)
2022-01-24 01:11:20	192.168.1.51	192.168.1.31	Modbus_Read.Holding.Registers	✓ 1.29 GB / 2.51 GB	OT-VLAN10_마이크로 세그먼트 (13)
2022-01-24 01:09:20	192.168.1.51	192.168.1.31	Modbus_Read.Holding.Registers	✓ 1.29 GB / 2.51 GB	OT-VLAN10_마이크로 세그먼트 (13)
2022-01-24 01:07:20	192.168.1.51	192.168.1.31	Modbus_Read.Holding.Registers	✓ 1.29 GB / 2.50 GB	OT-VLAN10_마이크로 세그먼트 (13)
2022-01-24 01:05:20	192.168.1.51	192.168.1.31	Modbus_Read.Holding.Registers	✓ 1.29 GB / 2.50 GB	OT-VLAN10_마이크로 세그먼트 (13)
2022-01-24 01:03:20	192.168.1.51	192.168.1.31	Modbus_Read.Holding.Registers	✓ 1.29 GB / 2.50 GB	OT-VLAN10_마이크로 세그먼트 (13)



2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

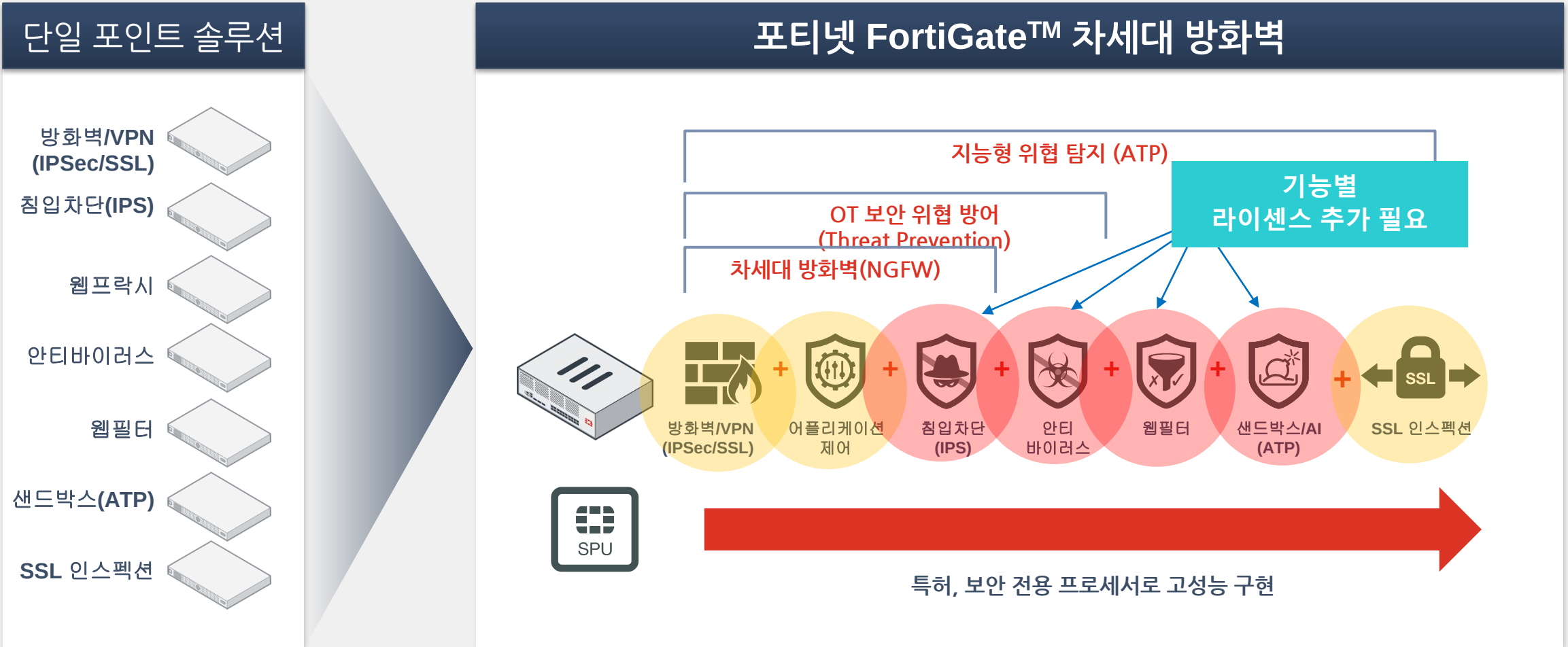
3) 네트워크 트래픽 통제 : FortiGate NGFW(UTM)



- 제조환경/ 공장 인프라환경에 필요한 기능이 포티넷 FortiGate 방화벽에 통합

2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

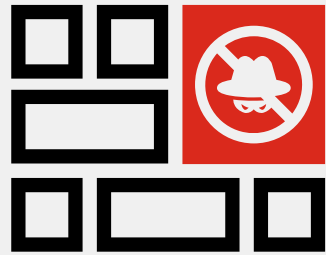
3) 네트워크 트래픽 통제 : FortiGate NGFW(UTM)



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

2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

3) 네트워크 트래픽 통제 : FortiGate NGFW(UTM)



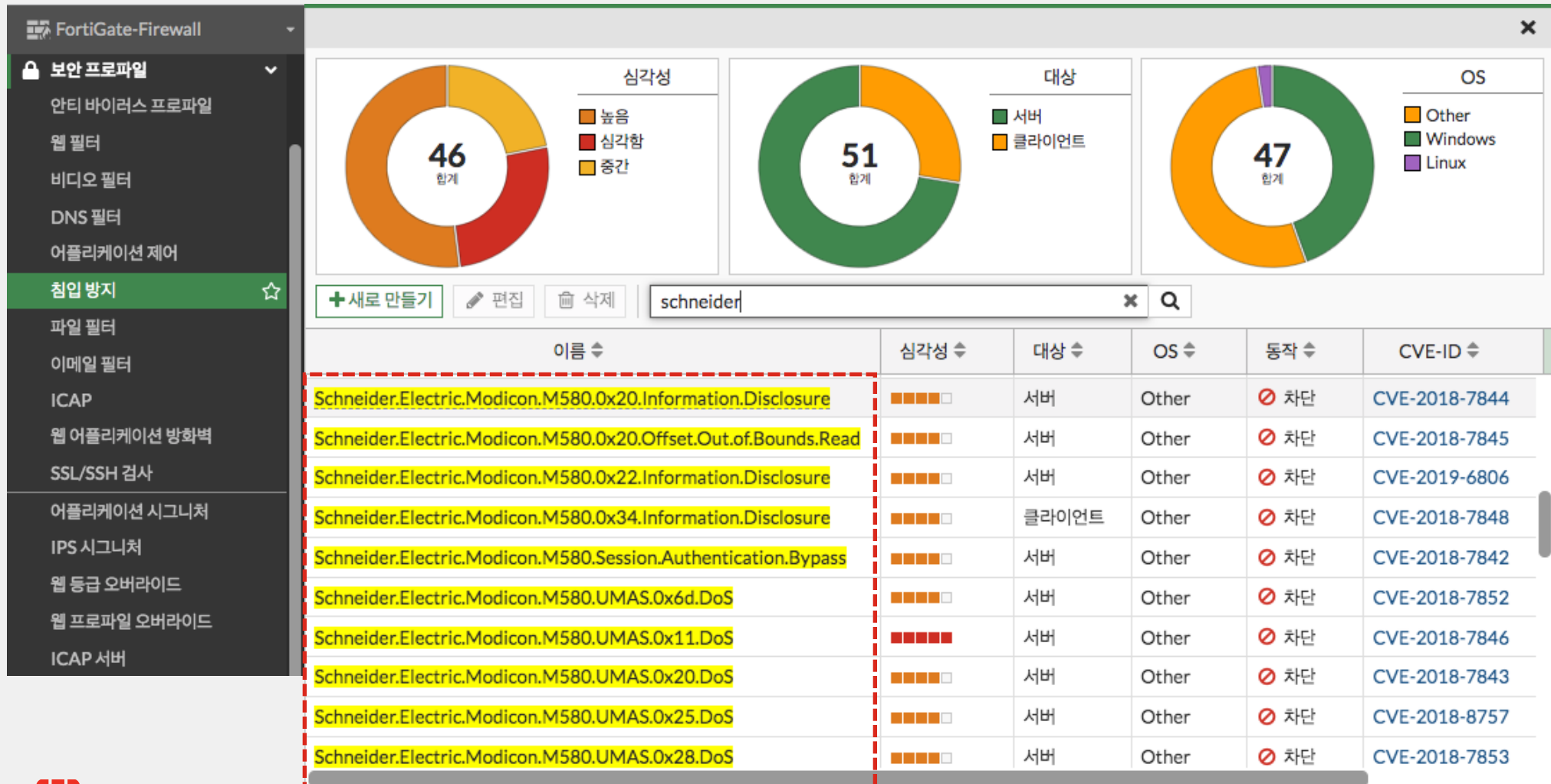
**ICS-CVE
(IPS)**

보안 취약점이 발견된 OT 제조사 장비

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

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
```

[illegible]

컨베이어벨트 정상 동작



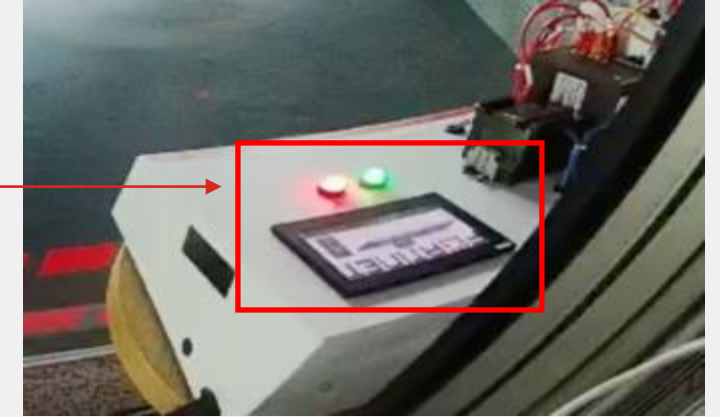
Date/Time	Source	Destination	Application Name	Action	Application User	Application Details
2020/10/17 11:41:16	192.168.14.13	192.168.1.4	Modbus_Read.Holding.Registers	pass		Read Holding Registers
2020/10/17 11:41:16	192.168.14.13	192.168.1.4	Modbus_Read.Holding.Registers	pass	192.168.14.13	Read Holding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



FortiGateRugged 90D FGR90DT618000045										
Action: 1 dropped Add Filter										
Date/Time	Severity	Source	Destination	Protocol	Destination Port	Service	Action	Attack Name		
2020/10/17 11:49:47	High	192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCPWrite.Request.PLC		
2020/10/17 11:40:58	High	192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCPUnauthorized.Read.Request.PLC		
2020/10/17 11:40:32	High	192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCPUnauthorized.Read.Request.PLC		
2020/10/16 17:02:52	High	192.168.14.4	192.168.1.45	6	502	MODBUS	detected	Modbus.TCPWrite.Request.PLC		
2020/10/16 17:01:36	High	192.168.14.4	192.168.1.45	6	502	MODBUS	detected	Modbus.TCPUnauthorized.Read.Request.PLC		
2020/10/16 16:57:23	High	192.168.14.4	192.168.1.44	6	502	MODBUS	detected	Modbus.TCPUnauthorized.Read.Request.PLC		
2020/10/16 14:20:45	High	192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCPWrite.Request.PLC		
2020/10/16 14:17:20	High	192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCPWrite.Request.PLC		
2020/10/16 14:16:22	High	192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCPWrite.Request.PLC		
2020/10/16 14:12:00	High	192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCPWrite.Request.PLC		
2020/10/16 14:11:24	High	192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCPWrite.Request.PLC		
2020/10/16 14:11:04	High	192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCPWrite.Request.PLC		
2020/10/16 14:10:46	High	192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCPWrite.Request.PLC		
2020/10/16 14:10:26	High	192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCPWrite.Request.PLC		
2020/10/16 14:10:23	High	192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCPWrite.Request.PLC		
2020/10/15 16:13:23	High	192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCPWrite.Request.PLC		
2020/10/15 16:13:06	High	192.168.14.13	192.168.1.4	6	502	MODBUS	detected	Modbus.TCPUnauthorized.Read.Request.PLC		



2. 제조환경/ 공장에 적합한 포티넷 솔루션 소개

3) 네트워크 트래픽 통제 : FortiGate NGFW(UTM)

The screenshot displays the FortiGate Rugged 90D web interface. The left sidebar shows the navigation menu with 'Intrusion Prevention' selected. The main content area is divided into two sections:

IPS Filters: A table showing filter details. A filter named 'Application: SCADA' is highlighted with a red box, showing an action of 'Block' and a status of 'On'.

Log & Report: A table showing log entries. A red box highlights a series of entries where the action is 'dropped' and the attack name is 'Modbus.TCPWrite.Request.PLC'.

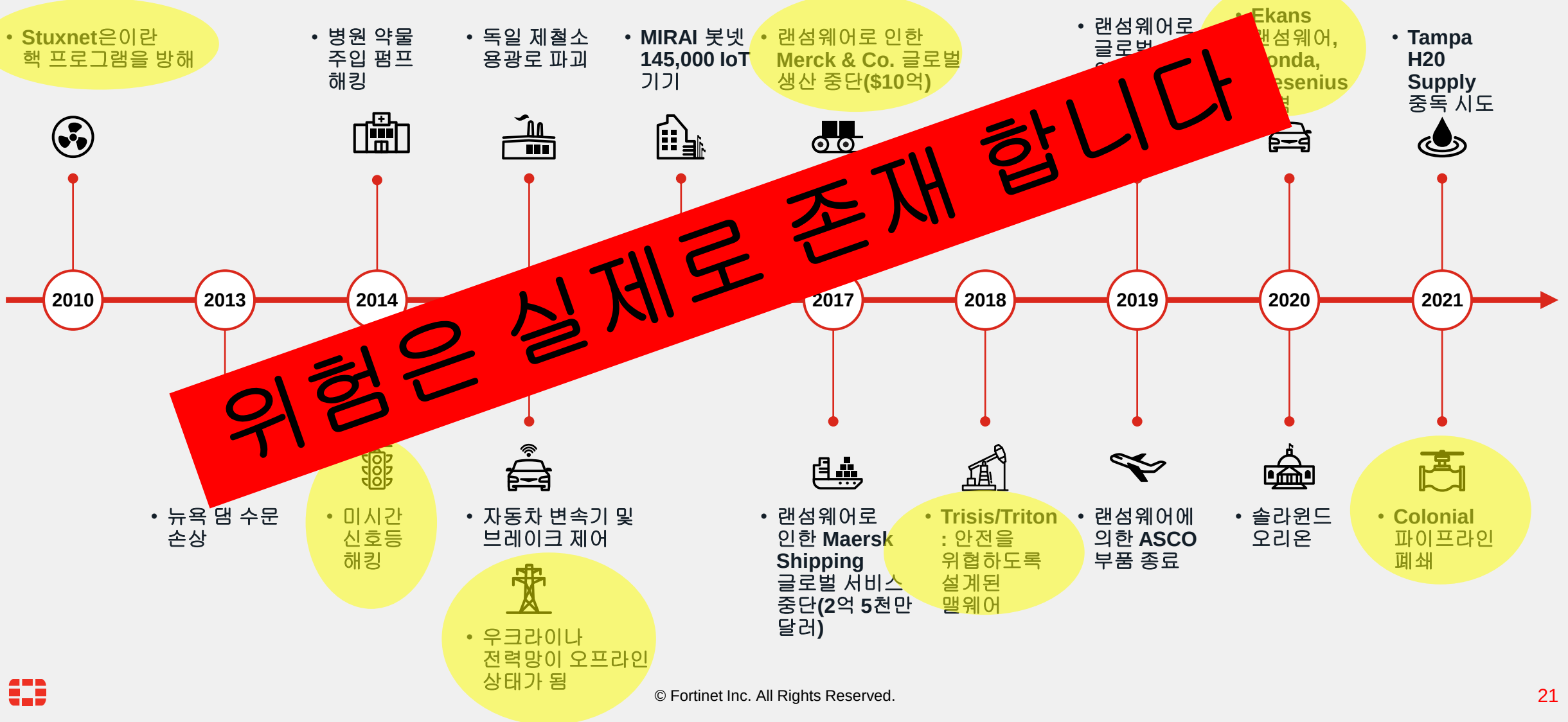
Date/Time	Severity	Source	Destination	Protocol	Destination Port	Service	Action	Attack Name
2020/10/17 12:28:16	High	192.168.14.13	192.168.1.4	6	502	MODBUS	dropped	Modbus.TCPWrite.Request.PLC
2020/10/17 12:27:57	High	192.168.14.13	192.168.1.4	6	502	MODBUS	dropped	Modbus.TCPWrite.Request.PLC
2020/10/17 12:27:36	High	192.168.14.13	192.168.1.4	6	502	MODBUS	dropped	Modbus.TCPWrite.Request.PLC
2020/10/17 12:27:33	High	192.168.14.13	192.168.1.4	6	502	MODBUS	dropped	Modbus.TCPWrite.Request.PLC
2020/10/16 14:20:24	High	192.168.14.13	192.168.1.4	6	502	MODBUS	dropped	Modbus.TCPWrite.Request.PLC
2020/10/16 14:20:04	High	192.168.14.13	192.168.1.4	6	502	MODBUS	dropped	Modbus.TCPWrite.Request.PLC
2020/10/16 14:19:46	High	192.168.14.13	192.168.1.4	6	502	MODBUS	dropped	Modbus.TCPWrite.Request.PLC
2020/10/16 14:19:28	High	192.168.14.13	192.168.1.4	6	502	MODBUS	dropped	Modbus.TCPWrite.Request.PLC
2020/10/16 14:19:08	High	192.168.14.13	192.168.1.4	6	502	MODBUS	dropped	Modbus.TCPWrite.Request.PLC
2020/10/16 14:19:04	High	192.168.14.13	192.168.1.4	6	502	MODBUS	dropped	Modbus.TCPWrite.Request.PLC

컨베이어벨트 정상 동작



3. 랜섬웨어 및 악성코드 탐지/차단 솔루션

- FortiSandbox / FortiAI / FortiEDR



3. 랜섬웨어 및 악성코드 탐지/차단 솔루션

- FortiSandbox / FortiAI / FortiEDR

FortiSandbox 2000E

File On-Demand

What are you looking for?

Dashboard

FortiView

Network

System

Virtual Machine

Scan Policy

Scan Input

File On-Demand

URL On-Demand

Job Queue

Sniffer

Device

FortiClient

Adapter

Network Sniffer

Quarantine

Malware Package

High Risk Ransomware

Overview

Tree View

Details

Basic Information

Job ID: 5892756464205765936

Status: Done

Received: Jan 24 2022 14:52:47

Started: Jan 24 2022 14:52:56+09:00

Rated By: VM Engine (AI)

Submit Type: On-Demand

Digital Signature: No

AI Mode: ON

SIMNET: OFF

Timeout Value: 180 seconds

Virus Total: [Q](#)

Details Information

Filename: db349b97c37d22f5ea1d1841e3c89eb4_Taiwan TSMC Wannacry

Downloaded From: db349b97c37d22f5ea1d1841e3c89eb4_Taiwan TSMC Wannacry

Scan Start Time: Jan 24 2022 14:52:56+09:00

Scan End Time: Jan 24 2022 14:56:18+09:00

Total Scan Time: 202 seconds

File Type: exe

VM Scan Start Time: Jan 24 2022 14:52:59+09:00

VM Scan End Time: Jan 24 2022 14:54:41+09:00

VM Scan Time: 102 seconds

File Size: 3723264 (bytes)

Embedded URL: 0

MD5: db349b97c37d22f5ea1d1841e3c89eb4

SHA1: e889544aff85ffaf8b0d0da705105dee7c97fe26

SHA256: 24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c

Action

monitored

analytics

analytics

blocked

monitored

analytics

analytics

blocked

analytics

blocked

monitored

analytics

analytics

blocked

analytics

blocked

monitored

analytics

analytics

blocked

analytics

blocked



3. 랜섬웨어 및 악성코드 탐지/차단 솔루션

- FortiSandbox / FortiAI / FortiEDR

FortiAI 3500F FAI35FT319000019

Dashboard

Security Fabric

Attack Scenario

Host Story

Virtual Security Analyst

Express Malware Analysis

Outbreak Search

Static Filter

Threat Investigation

Network

System

User & Device

Log & Report

Back Information View Investigator View

Add To Allow List

VSA Verdict : Critical Risk

 **Industroyer**

Industroyer is modular malware which designed to disrupt the working processes of industrial control systems, specifically those used in electrical substations.

Confidence level: 100.00%

Sample Information

File ID 78179

Submitted Date 2022/01/24 14:42:12 Last Analyzed 2022/01/24 14:42:14

File Type PE File Size 26616(26.0 KB)

File Name f8153747bae8b4ae48837ee17172151e_Stuxnet MD5 f8153747bae8b4ae48837ee17172151e VT f8153747bae8b4ae48837ee17172151e

SHA256 1635ec04f069ccc8331d01fdf31132a4bc8f6fd3830ac94739df95ee093c555c

SHA1 cb0793029c60c0bd059ff85de956619f7fdeb4fd

Detection Name W32/Stuxnet.A!tr.rkit Virus Family N/A

Source Device

Device Type Manual Upload

Network

This file was manually submitted to Virtual Security Analyst for analysis.

Feature Composition



Feature Type Appearance In Sample

Industroyer 1

History

Search

Date	MD5	File Type	Detection Name	Device	VDOM	Attacker	Victim	Confidence Level	Risk Level
2022/01/24 14:42:12	f8153747bae8b4ae48837ee17172151e	PE	W32/Stuxnet.A!tr.rkit	Manual Upload	N/A	N/A	N/A	High (100.0%)	Critical
2021/12/09 18:35:25	f8153747bae8b4ae48837ee17172151e	PE	W32/Stuxnet.A!tr.rkit	FortiGate-Firewall	root	192.168.5.44	192.168.14.71	High (100.0%)	Critical
2021/12/09 16:58:54	f8153747bae8b4ae48837ee17172151e	PE	W32/Stuxnet.A!tr.rkit	Other Device	global	192.168.5.44	192.168.14.71	High (100.0%)	Critical
2021/11/21 01:55:41	f8153747bae8b4ae48837ee17172151e	PE	W32/Stuxnet.A!tr.rkit	Manual Upload	N/A	N/A	N/A	High (100.0%)	Critical



3. 랜섬웨어 및 악성코드 탐지/차단 솔루션

- FortiSandbox / FortiAI / FortiEDR

The screenshot displays the Fortinet FortiEDR interface. The top navigation bar includes sections like DASHBOARD, EVENT VIEWER, FORENSICS, COMMUNICATION CONTROL, SECURITY SETTINGS, INVENTORY, and ADMINISTRATION. The main area is divided into 'APPLICATIONS' and 'APPLICATION DETAILS'.

APPLICATIONS

At the top, there's a filter bar with 'If Vendor is within' and a dropdown menu. Below this is a table of applications. A red box highlights the first row: 'Host Process for Windows Services' by Microsoft Corporation, with a reputation of 'Unknown' and a vulnerability of 'Unknown'. Other rows show various system processes like '10.0.18362.1 (WinBuild.1...', '10.0.14393.0 (rs1_release...', '10.0.19041.1 (WinBuild.1...', '10.0.19041.546 (WinBuild...', '6.1.7600.16385 (win7_rtm...', 'Microsoft Office', 'Speech Model Download Execu...', 'MS Connection Broker', and 'Microsoft Windows Host'.

APPLICATION DETAILS

On the right, the 'APPLICATION DETAILS' section shows 'Host Process for Windows Services'. It includes a 'Policies' table with columns 'Policy' and 'Action'. The policies listed are 'Default Communication Control ...', 'Servers Policy', and 'Isolation Policy', all with an 'Allow' action.

ADVANCED DATA

At the bottom, the 'ADVANCED DATA' section is divided into three parts: 'APPLICATION INFO', 'APPLICATION USAGE', and 'DESTINATIONS'. 'APPLICATION INFO' shows details like 'Application Description: Host Process for Windows Services', 'First Connection Time: 08-Jul-2020, 06:32:44', 'Last Connection Time: 02-Jun-2021, 04:17:01', and 'Process Names: %Device%HarddiskVolume4%Windows%System32%svchost.exe (75C5A97F5...', '%Device%HarddiskVolume1%Windows%System32%svchost.exe (619652B42...', and 'And 3 more...'. 'APPLICATION USAGE' shows 'Total System: 1839.0 connections / day', 'yuhanchem: 552.4 connections / day', and 'Default Collector Group: 1708.6 connections / day'. 'DESTINATIONS' shows a table with columns 'IP', 'CONNECTION TIME', and 'COUNTRY', listing connections to Singapore and United States.

Annotations:

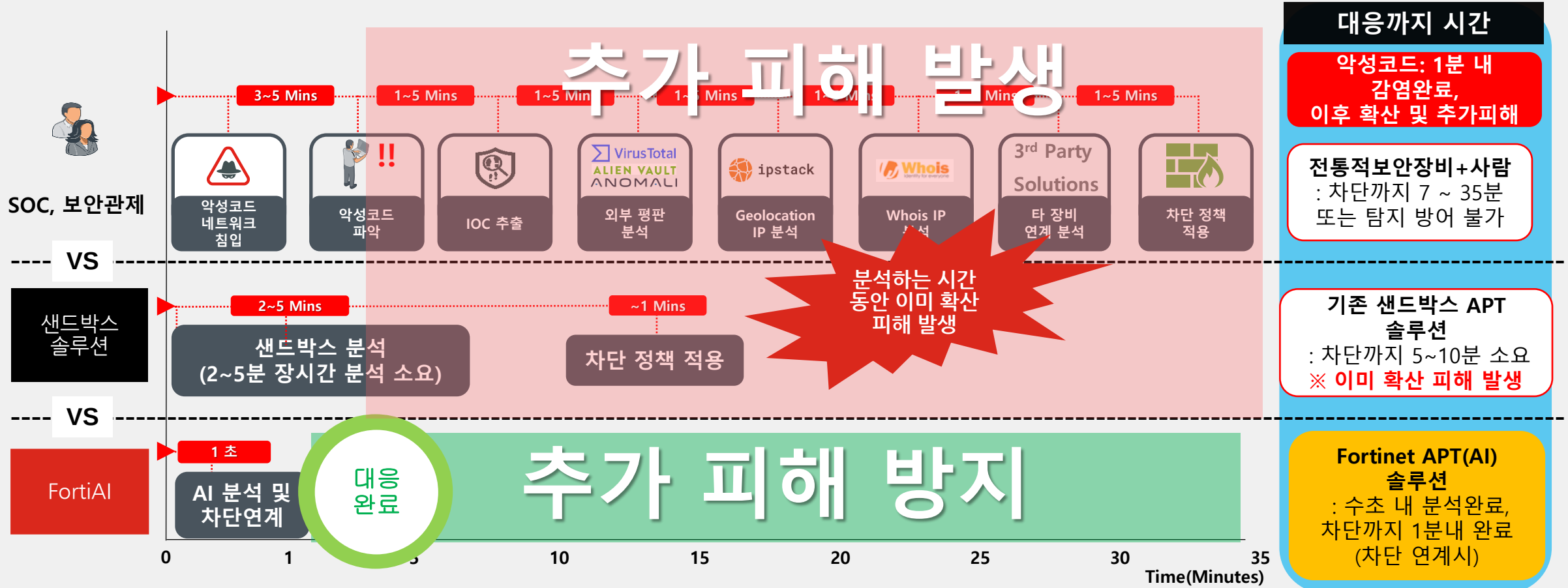
- 엔드포인트에 설치된 어플리케이션 확인 (Check applications installed on endpoints)
- 엔드포인트에서 실행되는 어플리케이션의 확인과 취약한 버전의 실행 차단 설정 (Check applications running on endpoints and set up blocking of execution of vulnerable versions)
- 어플리케이션에 대한 통제정책 확인 (Check control policies for applications)
- 어플리케이션 평판과 취약성 확인 (Check application reputation and vulnerability)



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

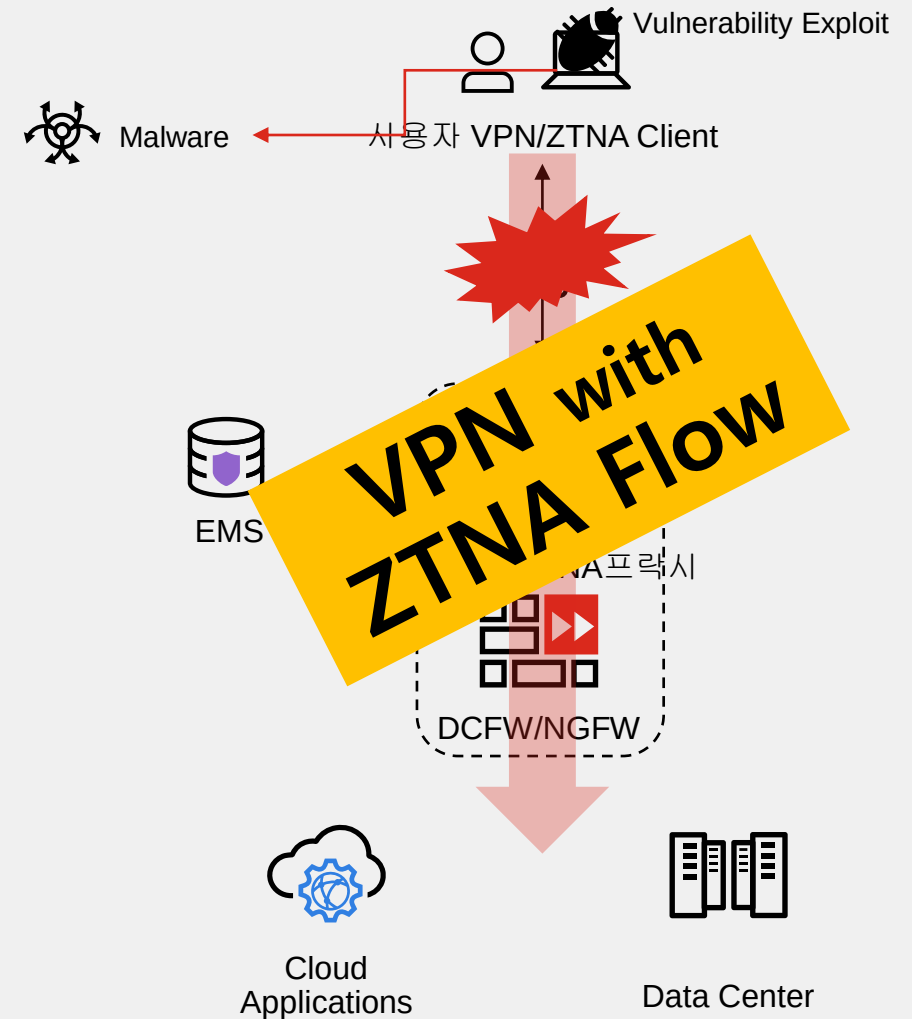
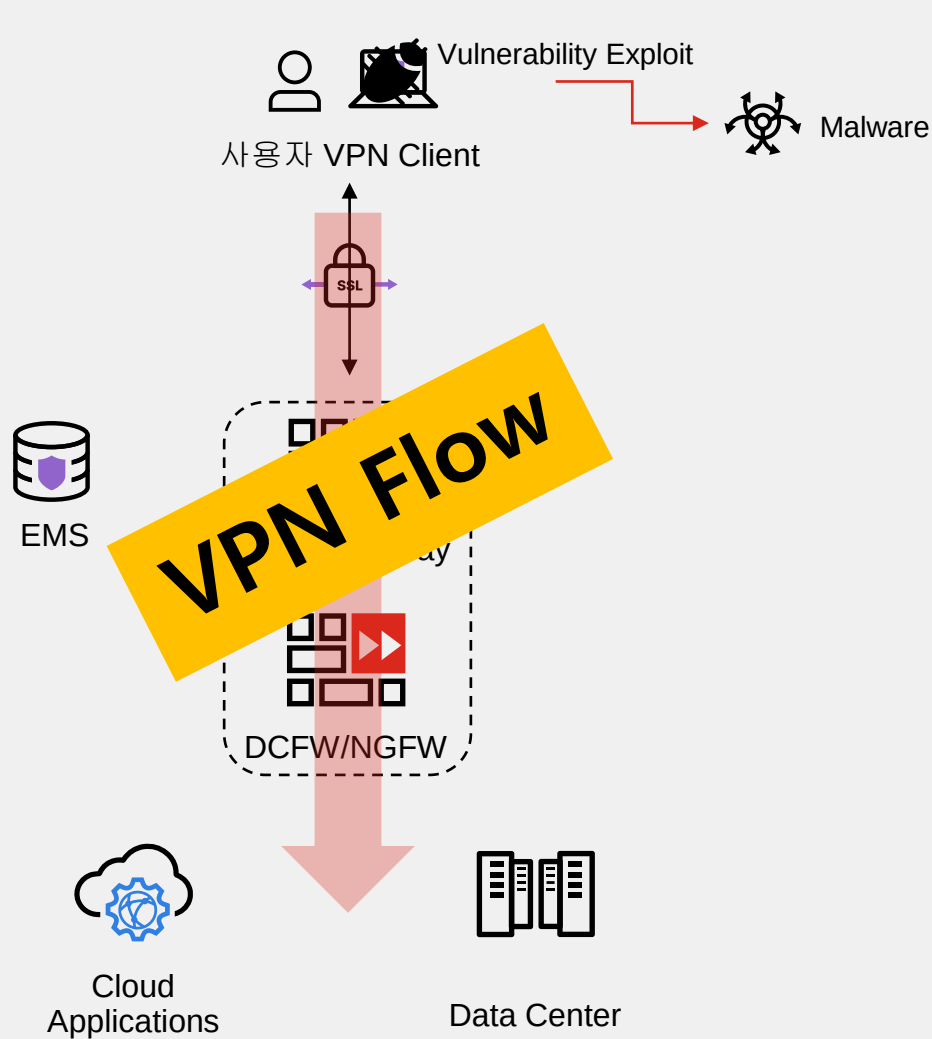
- 제로트러스트(ZTNA) 태그 룰
 - Windows 10
 - Anti-Virus 설치

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

FortiClient Endpoint Management Server

SSL Certificate is not secure

Invitations

?

admin

Dashboard

Endpoints

Deployment & Installers

Endpoint Policy & Compone...

Endpoint Profiles

Zero Trust Tags

Zero Trust Tagging Rules

Zero Trust Tag Monitor

FortiGuard Outbreak Alerts

Software Inventory

Quarantine Management

Administration

System Settings

Zero Trust Tagging Rule Sets

Manage Tags

Import

Export

Add

Refresh

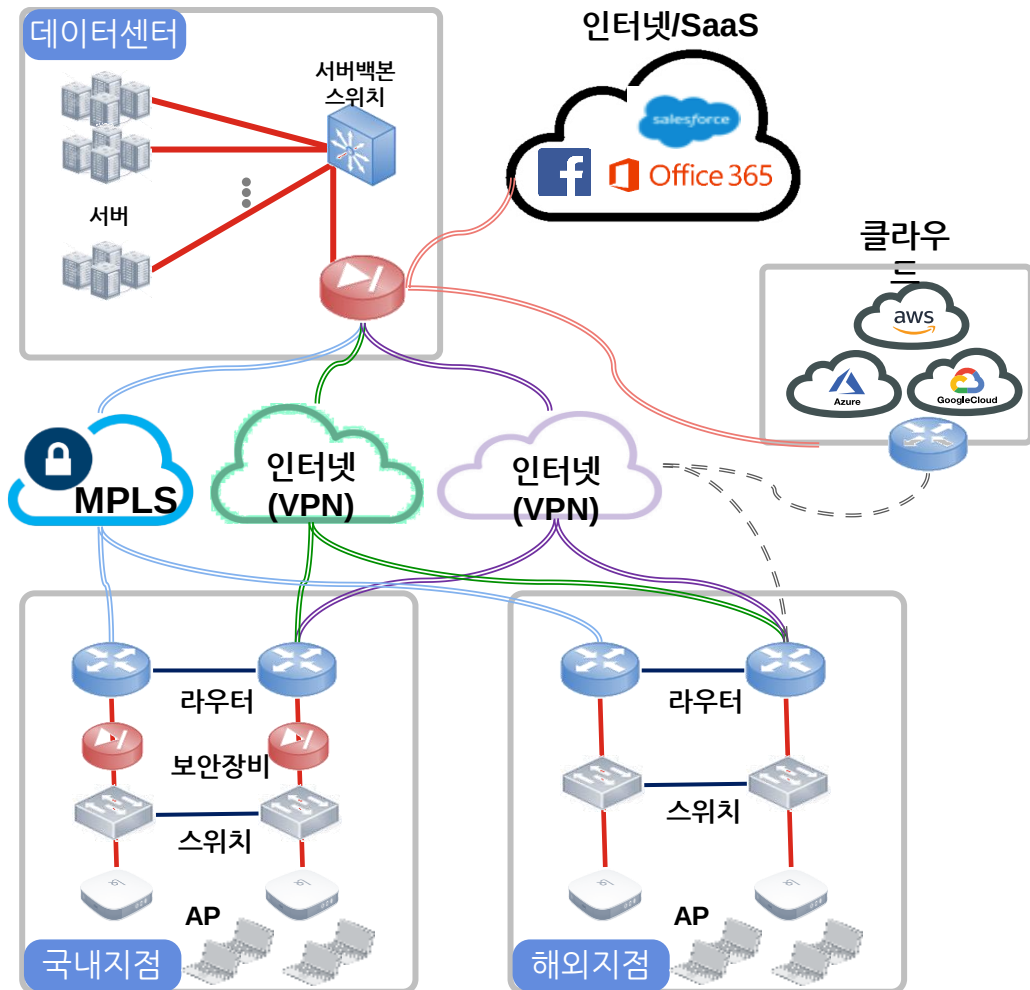
Clear Filters

Name	Tag	Enabled	Comments		
Add New Rule					
OS	Windows	Mac	Linux	iOS	Android
Rule Type	AD Group				
AD Group	☐ NOT No AD groups found				
SaveCancel					
OS 버전 확인OS 버전 확인Windows 10 이상					



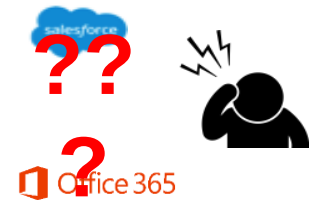
4. 안전한 VPN 접속 및 VPN 통신의 효율성 극대화 솔루션

- FortiGate SD-WAN



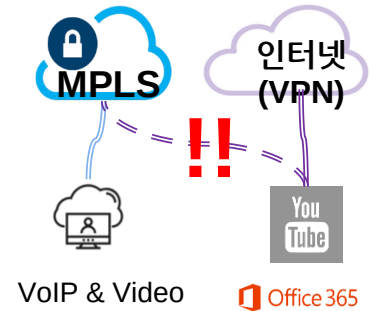
트래픽 가시성

네트워크상의 트래픽에 대한 가시성 부족



회선 대역폭의 효율적인 사용

모든 트래픽을 데이터센터의 보안 장비를 거쳐 통신, 어플리케이션별 라우팅 불가
대용량 트래픽의 MPLS 회선 사용



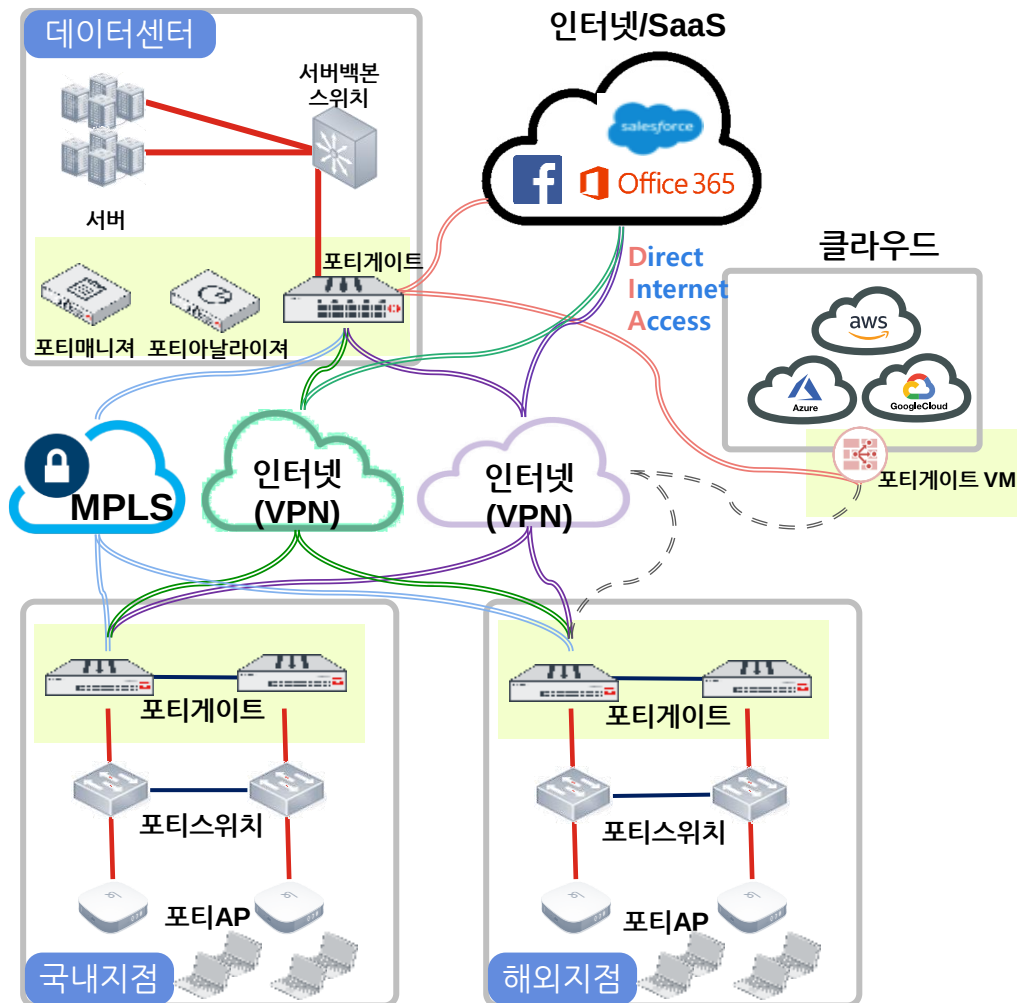
Cloud 및 SaaS 접속

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



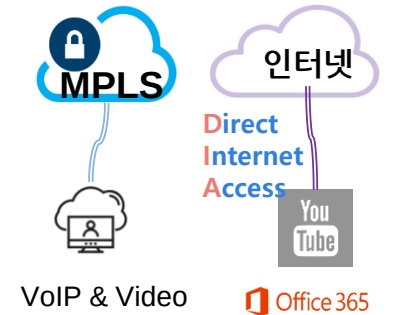
트래픽 가시성

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	Lowest Cost
2	Voice & Video	Internal IP address	Overlay(오버레이) VPN_1 VPN_2	Lowest Cost or Best Quality (Lab)
3	Business Critical 인터넷	Salesforce Microsoft O365	VPN_2 ISP 1	Lowest Cost
4	Business Non-critical 인터넷	Microsoft Update	Underlay/Overlay ISP_2 VPN_1	Lowest Cost (Lab) or Maximize BW
5	Non_business 인터넷	Other 인터넷	ISP_2	Manual
6	Implicit	Implicit	Underlay(언더레이) 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®