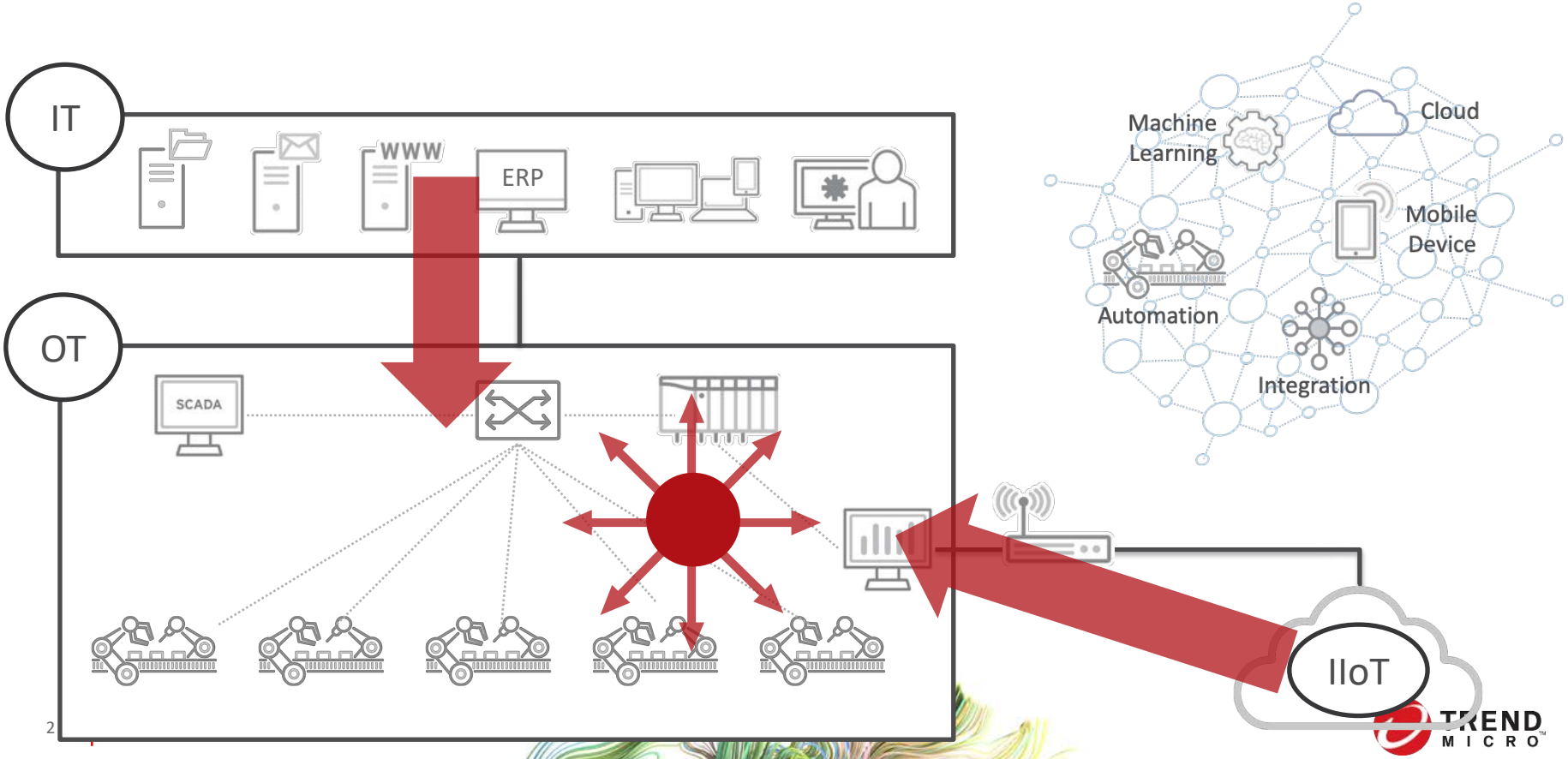
가용성을 보장하는 효과적인 OT보안 전략

장 성 민

Trend Micro

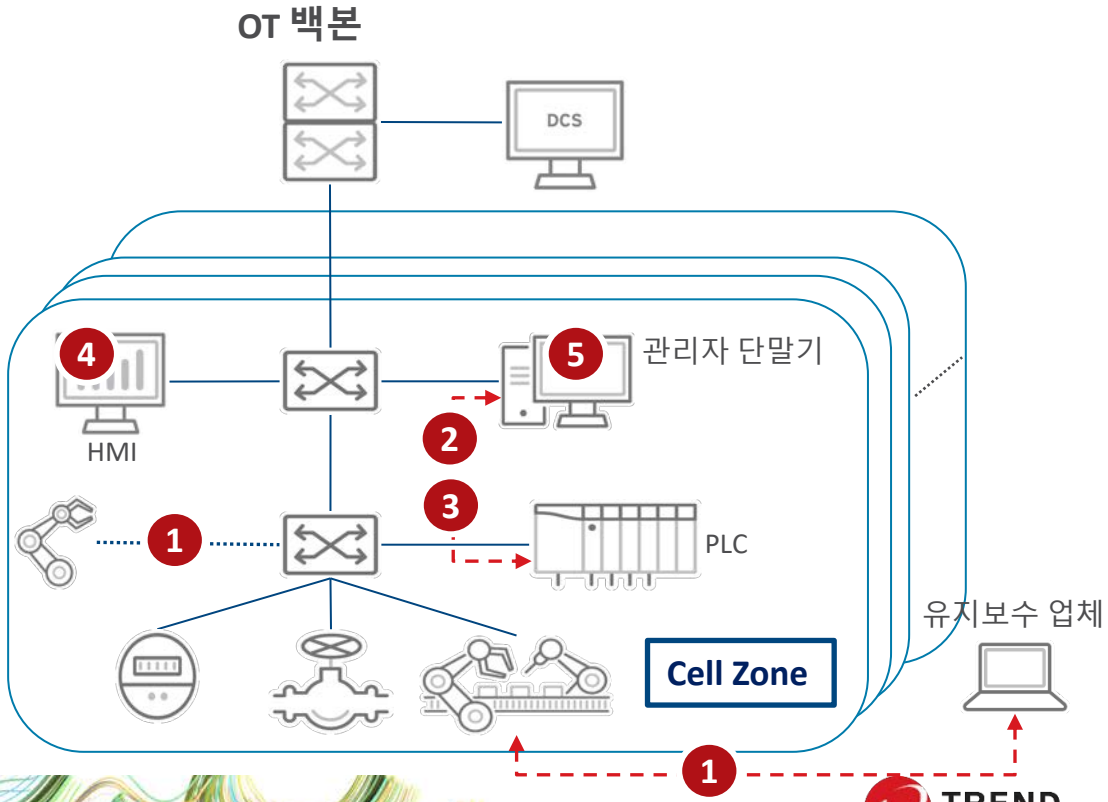
산업 시설 네트워킹, IT-OT 연계, IIoT



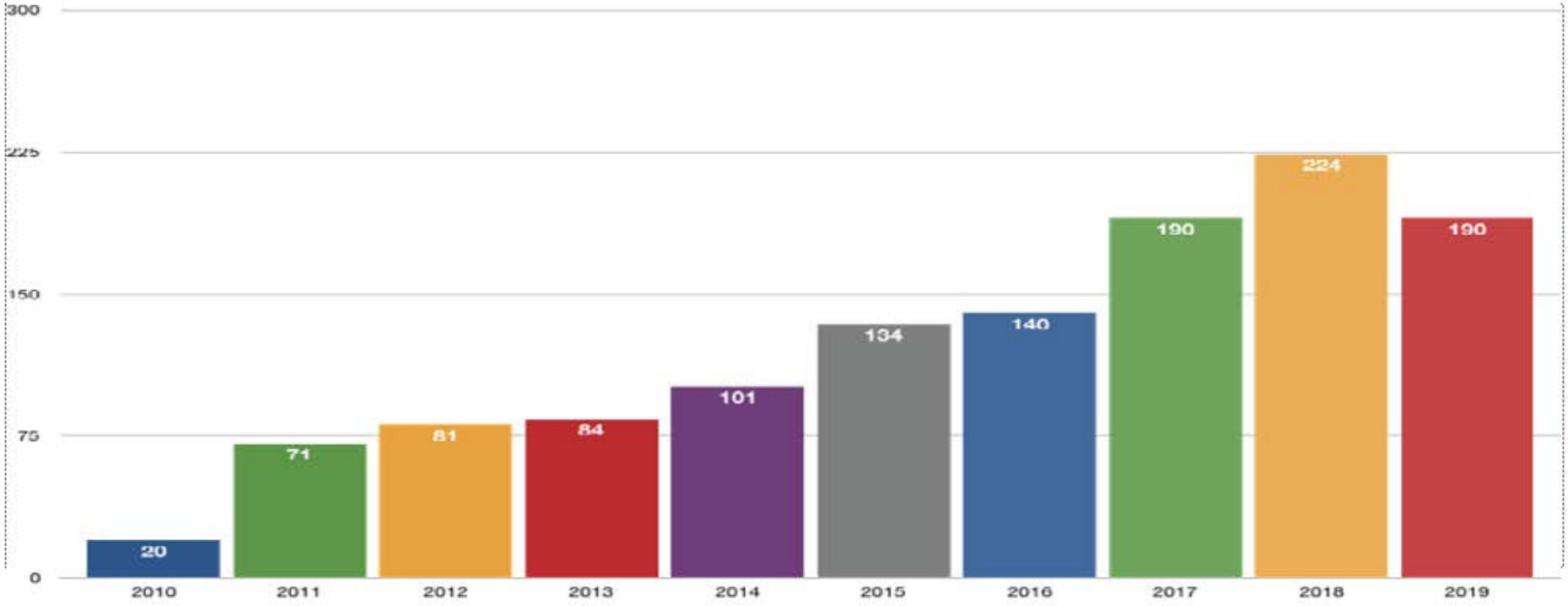
TREND MICRO

OT 보안 취약 요소

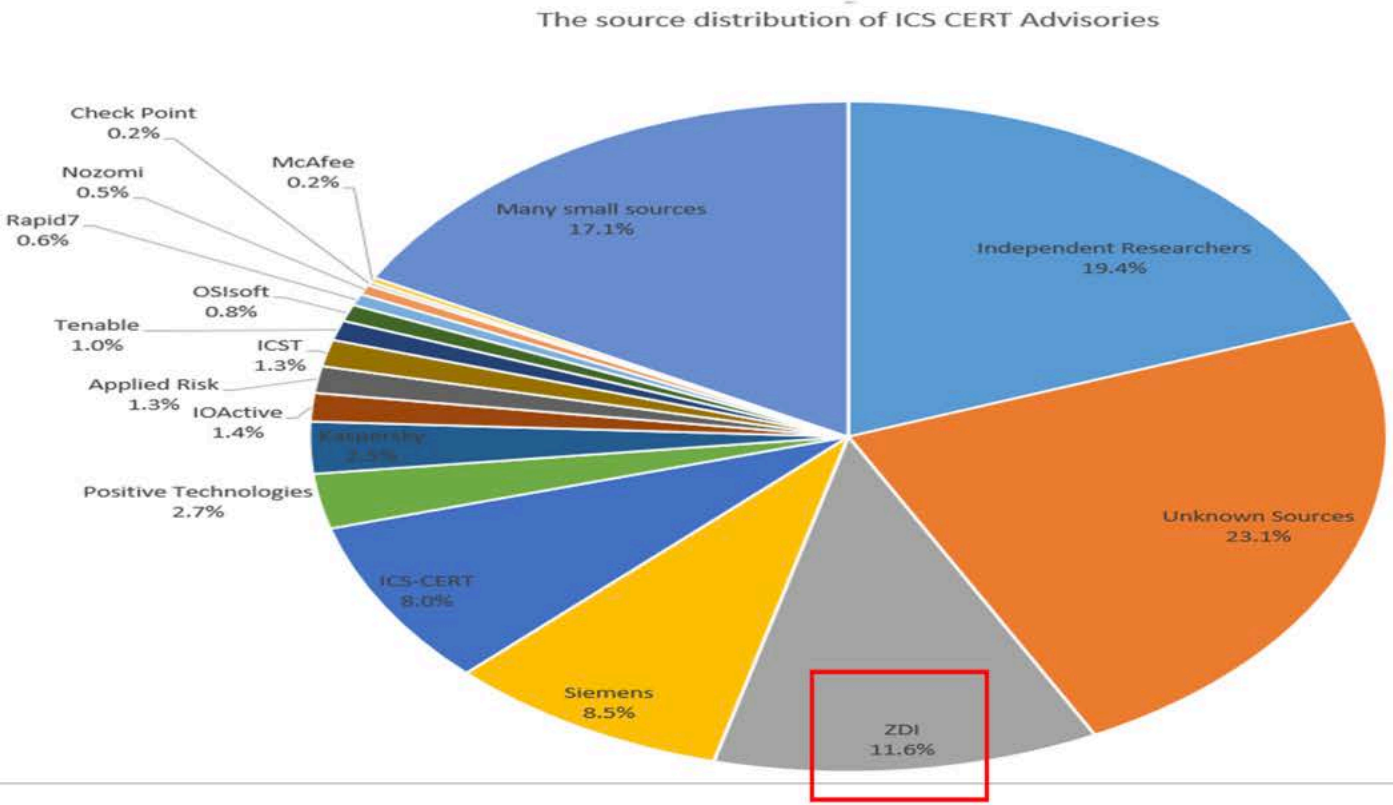
1. **관리되지 않는 OT 요소**
   - 관리되지 않는 디바이스 및 통신
2. **안전하지 않은 인증 방식**
   - 디바이스 디자인 및 구성에 따른 결함
3. **안전하지 않은 프로토콜**
   - 암호화 되지 않음
4. **패치되지 않은 디바이스**
   - 패치가 가능하지 않음
5. **안전하지 않은 3rd-Party S/W**
   - 초기 공급과정에서 보안 취약한 상태이거나 감염됨



The ICS vulnerability number per year. (Data source: ICS CERT, 2019/12/04)

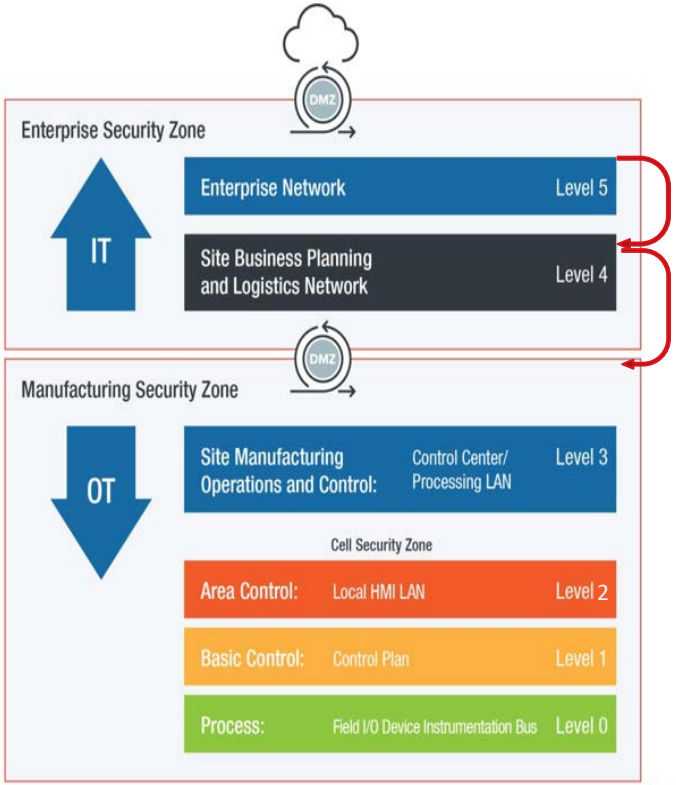


The contributor distribution of ICS CERT advisories
(source: ICS CERT, counting period: 2010-2019/12/04)



표적 공격과 랜섬웨어

침입 경로

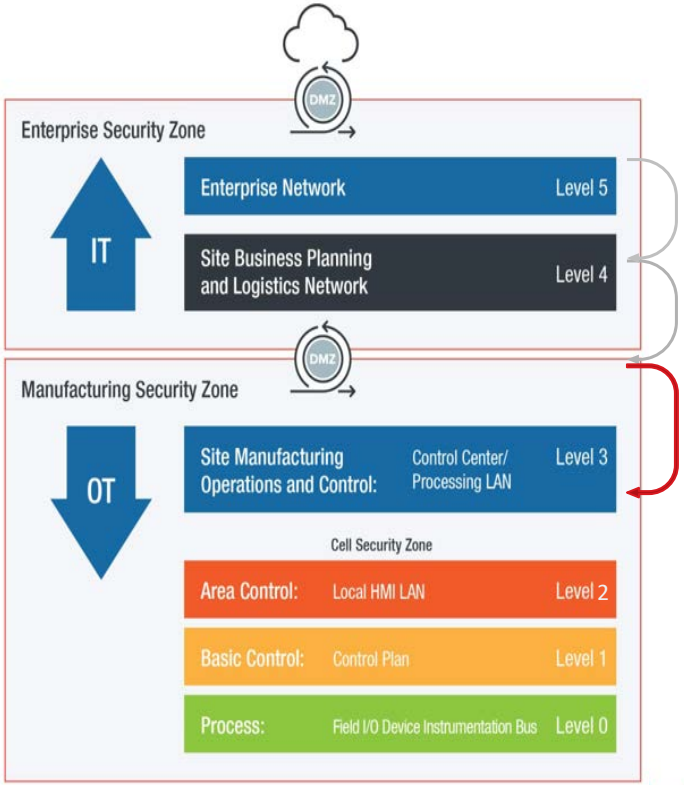


- 서버 취약점 또는 악성 이메일을 통한 IT 내부 침입.
- 서버 취약점이나 기밀 정보 탈취로 OT DMZ 침입.

표적 공격과 랜섬웨어

Reconnaissance
Exploit
Command and Control

침입 경로



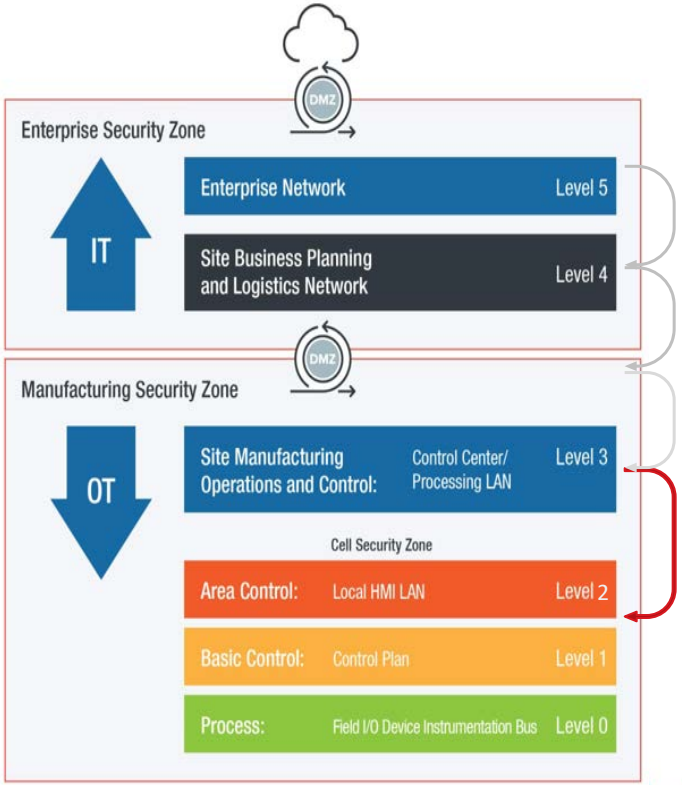
서버 취약점 또는 탈취한 정보를 통해 L3 Zone 접근. 이후,

- DNS, DHCP, AD등과 같은 OT 내부 인프라 공격.
- OT내 PC 기반 머신들의 정보 획득
- C&C 채널 연결

표적 공격과 랜섬웨어

Deliver
Install
Execute ICS Attack

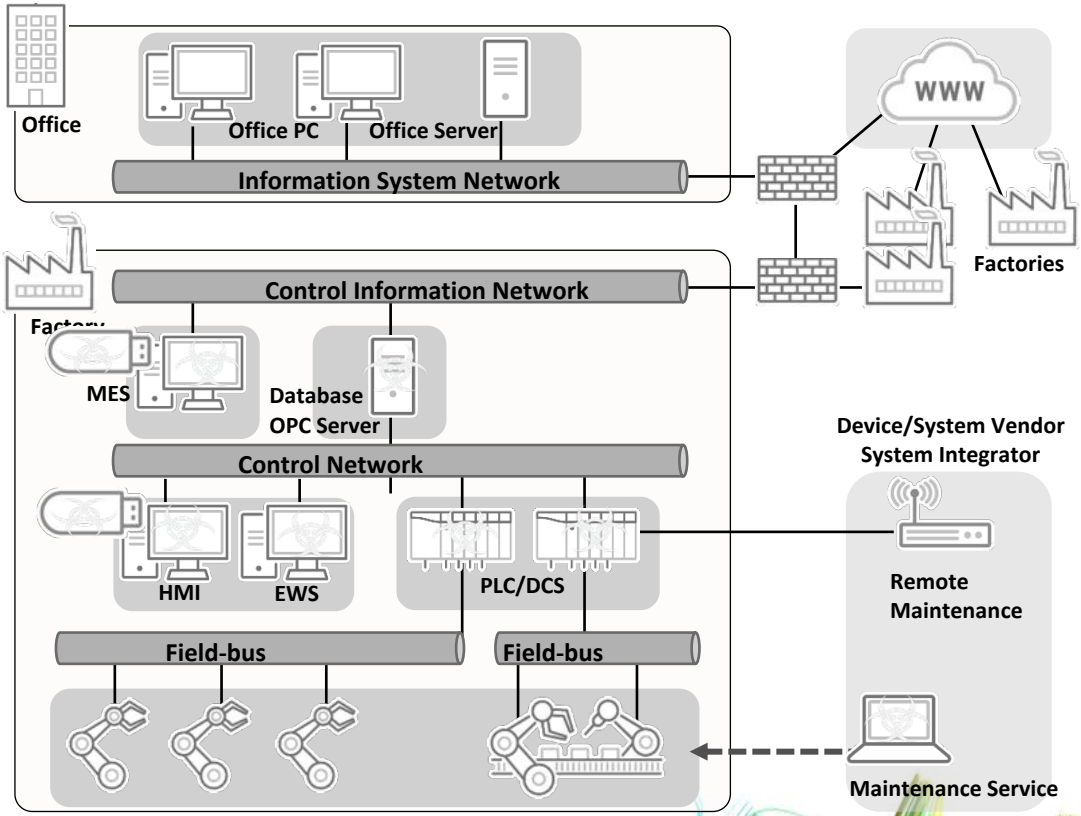
침입 경로



OT내 최하위 레벨까지 접근

- 지속적 공격을 위해 획득한 정보로 악성코드 또는 랜섬웨어 배포
- 생산 시설/서비스 파괴의 원인이 되는 HMIs/PLCs 취약점 공격
- 취약한 인증 처리로 오동작의 원인이 되는 HMIs/PLCs 제어

웜 공격(전파) - Non-Targeted Attack



외부 협력업체 또는 내부 직원의 노트북이나 USB 저장매체를 통해 감염/전파

Victim Companies	Impact
Pharmaceutical, chemical (German)	$310,000,000+
Multinational delivery services	$300,000,000+
Construction materials	$380,000,000+
Maritime	$300,000,000+
Semiconductor Manufacturing (Taiwan)	$250,000,000+

TREND MICRO

Best Practice

NIST 800-82 - Guide to Industrial Control Systems (ICS) Security

Method

ICS Risk Management and Assessment	ICS Security Program Development and Deployment	ICS Security Architecture	Applying Security Control to ICS
• Risk management process • Impact consideration	• Building business case and team for upper management support • Risk management framework implementation	• Network Segmentation • Network Segregation • Network NAT • Boundary Protection • Rule/Protocol policy •	• Applying Risk Assessment Framework in ICS • Guidance on Application of Security Control on ICS • .....

Security Objectives

1. Restricting logical access to the ICS network and network activity
2. Restricting physical access to the ICS network and devices
3. Protecting individual ICS components from exploitation
4. Restricting unauthorized modification of data
5. Detecting security events and incidents
6. Maintaining functionality during adverse conditions
7. Restoring the system after an incident

TREND MICRO

Trend Micro TXOne Solutions

가용성을 보장하는 OT 보안 솔루션

OT 환경과 운영에 가용성을 보장하는 보안 솔루션

쉬운 설치/배포

(랙 또는 캐비닛)

내구성 강한 하드웨어

(폭 넓은 온도 범위, 최고의 MTBF)

서비스 안정성 (하드웨어 이상/장애시에도 서비스/생산 라인 영향 없는 디자인)

SW 설치 필요 없음

(Malware 검사 필요 시스템)

간편한 사용

폐쇄망 환경 지원

랜섬웨어 방어

(허가 받지 않은 변조 방어)

비용 절감 (시스템 무결성 유지)

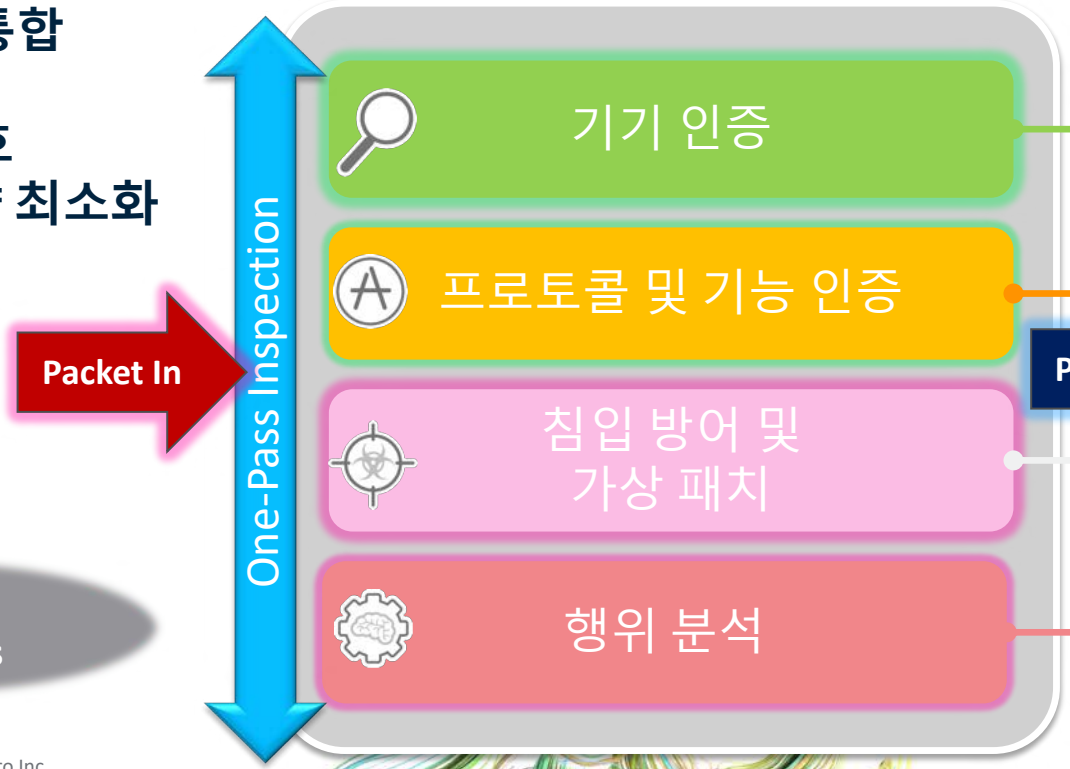
시스템 부하 최소

(적용된 시스템의 리소스 최소 사용)

TXOne Network Core Engine: TXODI™

-TXOne One-Pass DPI (산업용)

- IT-OT DNA 통합
- 가시성
- 제어 및 보호
- 서비스 영향 최소화



Latency
< 0.5 ms

Vendor ID
Device Type
Product Code
...

Protocols:
CC-Link
Modbus
Ethernet/IP
Profinet
...
Functions:
Read/Write/
Config/Reset/...

ICSA-19-017-01
ICSA-18-352-06
CVE-2018-8072
CVE-2018-8854
...

Connectivity
Type
Peer Type
Frequency

TXOne OT protocol support

EdgeFire FW 1.0

OT Protocol Granular Control (Basic.)	OT Protocol Granular Control (Advanced.)	OT Protocol Visibility & Detection
Modbus EthernetIP/CIP Siemens S7COMM Siemens S7COMM+ OMRON FINS MITSUBISHI-SLMP	Modbus	OPC UA Modbus EtherNet IP/CIP Niagara Fox BACnet SIEMENS S7Comm SIEMENS S7Comm Plus DNP3 HART-IP OMRON Fins Bechoff ADS IEEE C37.118 IEC 61850-5 MITSUBISHI-SLMP MELSOFT Modbus Schneider CC-LINK IE IEC 60870-5-104 FATEK PLC

Support OT protocol of **Power & Electricity**

OT protocol of granular control **(+ 2 Protocols in basic.) (+ 6 Protocols in adv.)**

Support OT protocol of visibility & Detections **(+ 19 Protocols in sig.)**

EdgeFire FW 1.1

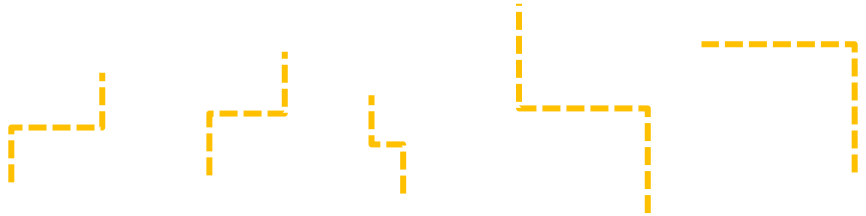
OT Protocol Granular Control (Basic.)	OT Protocol Granular Control (Advanced.)	OT Protocol Visibility & Detection
Modbus EthernetIP/CIP Siemens S7COMM Siemens S7COMM+ OMRON FINS MITSUBISHI-SLMP SECS/GEM IEC61850-MMS	Modbus EthernetIP/CIP Siemens S7COMM Siemens S7COMM+ MITSUBISHI-SLMP MELSOFT TOYUPUC	OPC UA Modbus EtherNet IP/CIP Niagara Fox BACnet SIEMENS S7Comm SIEMENS S7Comm Plus DNP3 HART-IP OMRON Fins Bechoff ADS IEEE C37.118 IEC 61850-5 MITSUBISHI-SLMP MELSOFT Modbus Schneider CC-LINK IE IEC 60870-5-104 FATEK PLC IEC 60870-5 (part of IEC 62351) IEC 61850 (part of IEC 62351) GOOSE OPC Classic(DA/AE/HAD) DICOM Health Level 7 TriStation Crimson CAN-ETH GE-SRTP via TCP Modbus Schneider Modicon Ladder Logic (Access) OpenSCADA User Interfaces (Access) Rapid SCADA User Interfaces (Access) EtherSBus (UDP) EtherSIO (UDP) Ethernet Powerlink (Access) Moxa Device Discovery (UDP) Advantech WebAccess SCADA Access (TCP)

TREND MICRO

! "#$%&'$

Model	EdgeFire-Formal Product (ICS Firewall)
CPU	Quad-Cores
LAN Interface	8*Copper ports (8 * 10/100/1G)
WAN Interface	2*Copper ports /2*ports SFP Fiber (Combo)
USB	Yes (USB X1)
Zero-Configuration	USB
Power input	Dual Power Input
Wide temperature	Yes(-40 to 75!C)
Throughput	200 Mbps +
Latency	<200 microseconds

Ruggedized hardware design



Giga Interface

Network Segmentation

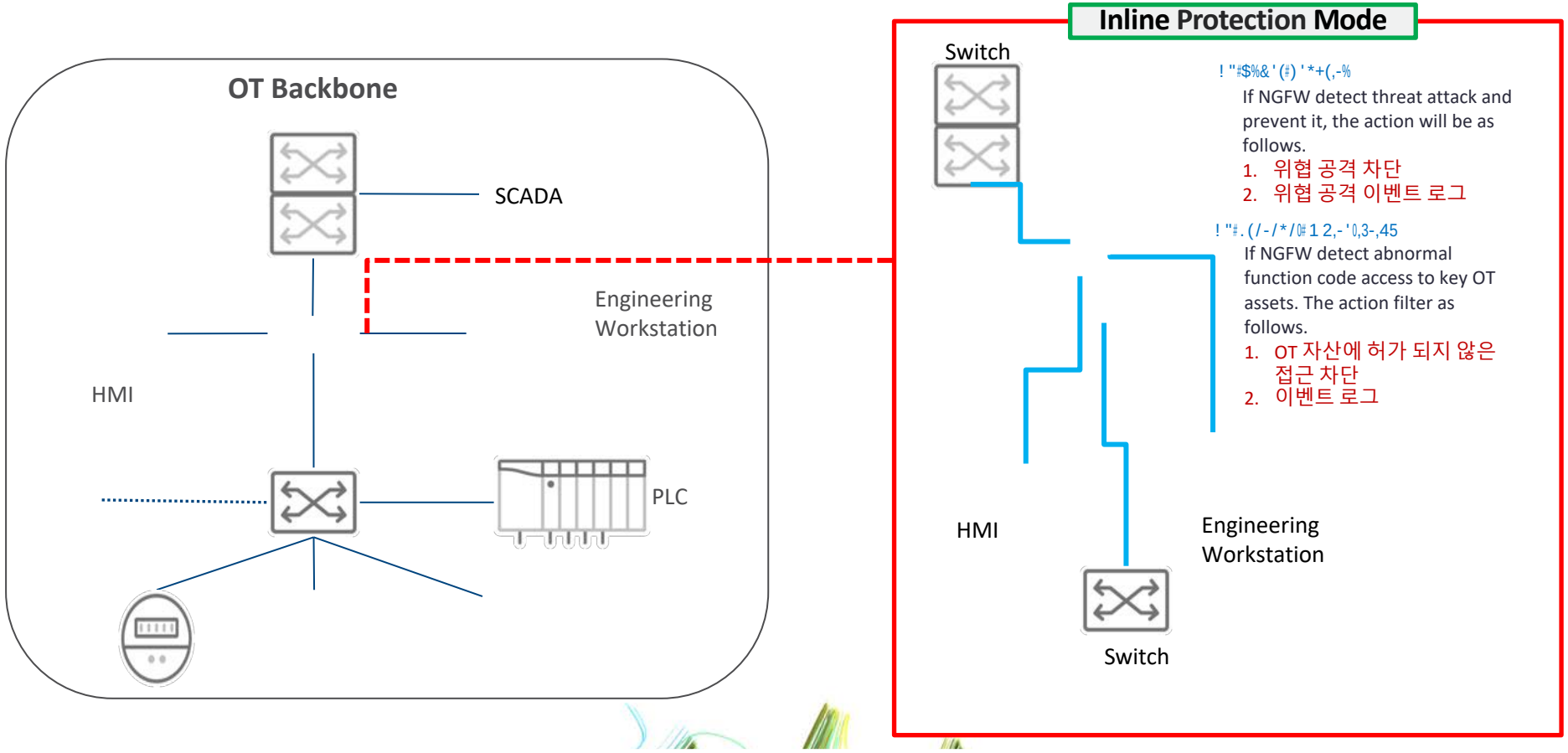
NAT

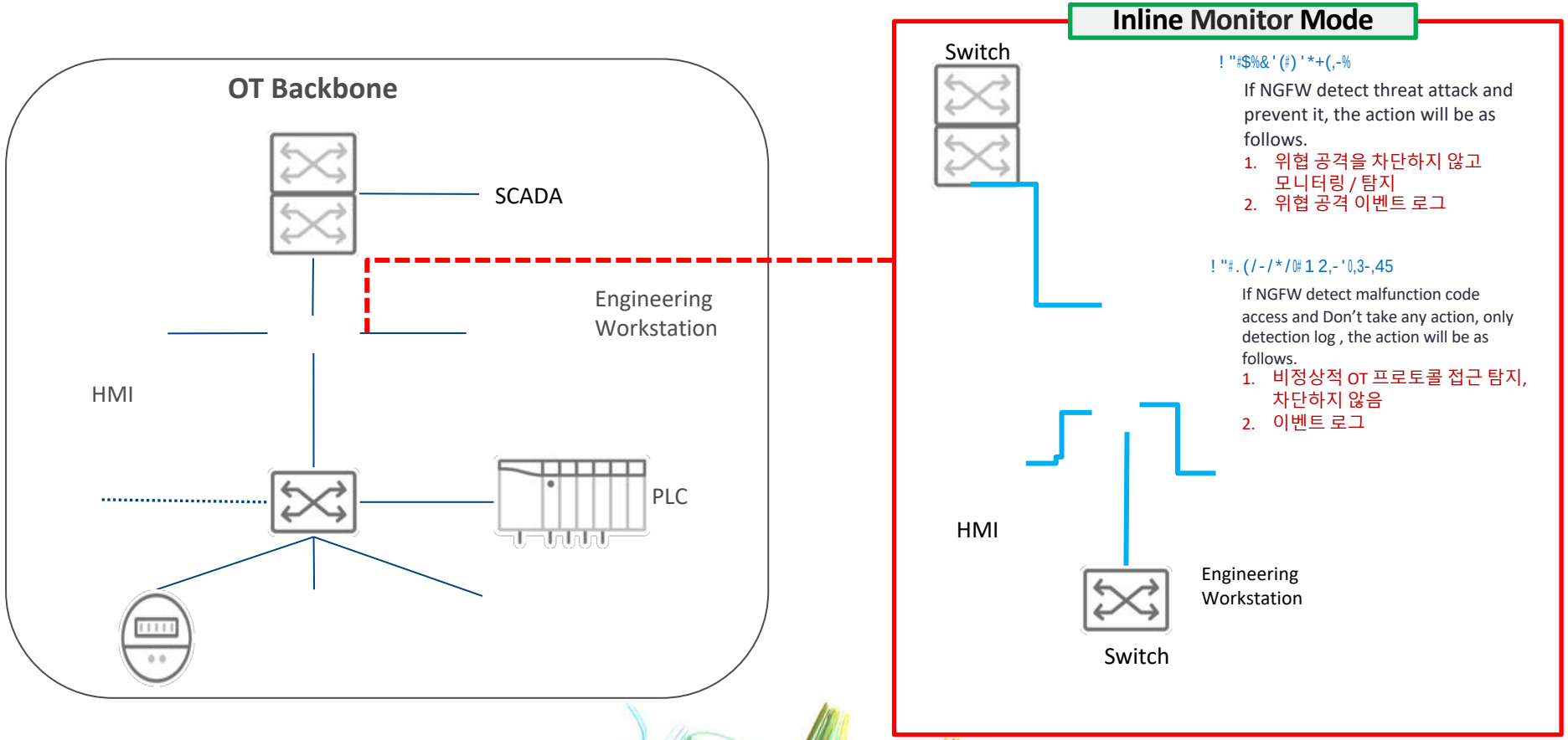
USB v2.0

Dual Power Input

Zero Configuration

TREND MICRO

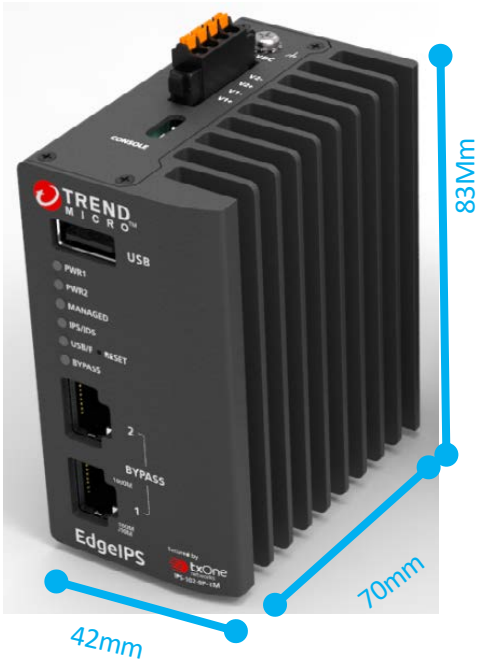

OT Backbone
SCADA
Engineering
Workstation
HMI
PLC
Inline Protection Mode
Switch
! "#$%&'(#) '*+(,-%
If NGFW detect threat attack and prevent it, the action will be as follows.
1. 위협 공격 차단
2. 위협 공격 이벤트 로그
! "#.(/-/*/0#12,-'0,3-,45
If NGFW detect abnormal function code access to key OT assets. The action filter as follows.
1. OT 자산에 허가 되지 않은 접근 차단
2. 이벤트 로그
HMI
Engineering
Workstation
Switch



EdgeIPS Series: Next-Generation Industrial IDPS

L2-L7 Visibility and Protection

- Network visibility
- Protocol Filter - Whitelisting Control
- Virtual Patch
- TXODI inside
- Hardware Bypass
- Dual Power input



Product name : EdgeIPS
Short name : IPS
Model name : IPS-102-BP-TM-T

(2 Copper ports + USB)

Formal Product

Protect mission-critical asset

- 중요한 자산 앞에 설치 (computers, HMI & controllers) 및 양방향 보호

Real IT-OT Integration

- OT 가시성과 제어 뿐 아니라 IT와 OT의 안전한 연계 구성을 위해 사이버 위협으로부터 보안 모니터링과 자산 보호를 제공
- ICS Protocol Filter.
- Hardware Bypass

Easy Management

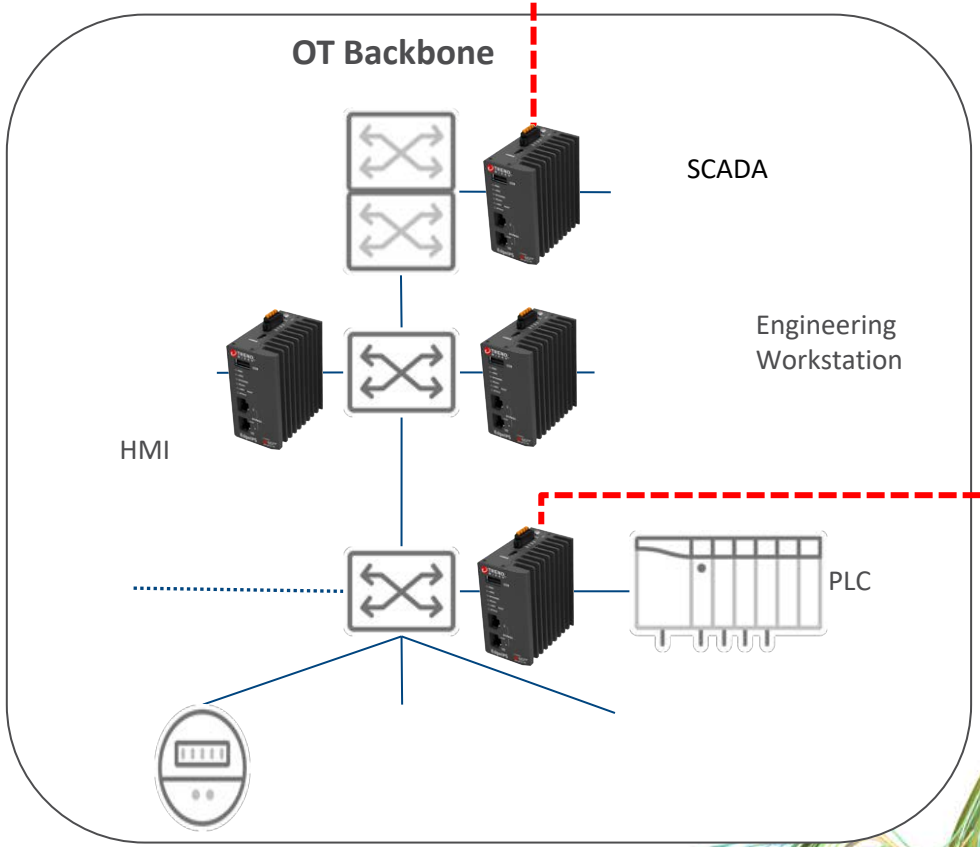
- OT Defense Console (ODC)로부터 중앙 관리
- 웹 콘솔로 모든 보안 노드의 통합 관리
- IP와 Network 서비스들을 위한 Object 기반 설정
- Zero-configuration

Robust System

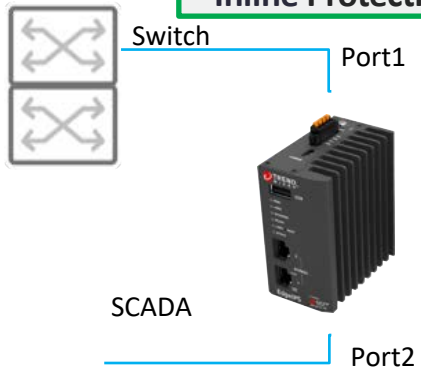
- High MTBF
- Dual power-Input
- -40 to 75°C wide temperature operation
- 5-years warranty
- Industrial grade hardware design
- Self-recovery watchdog
- *Wide Temperature (–40°C to 75°C)

Support both inline or passive Deployment

67(82/()*+,--,+&.)/*0$),'&./1()-&)$/2$03'&+4/9."$



Inline Protection mode



$%&'(#)'*+(,-%

If NGIPS detect threat attack and prevent it, the action will be as follows.

1. 위협 공격 차단
2. 위협 공격 이벤트 로그

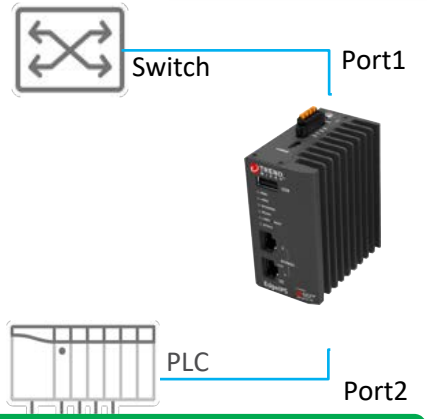
!"#.(/-/*/0#12,-'0,3-,45

If NGIPS detect malfunction code access key assets and will prevent it , the action will be as follows.

1. OT 자산에 허가 되지 않은 접근 차단
2. 이벤트 로그

Detection and blocking

Inline Monitor mode



$%&'(#)'*+(,-%

If NGIPS detect threat attack and Don't prevent it, the action will be as follows.

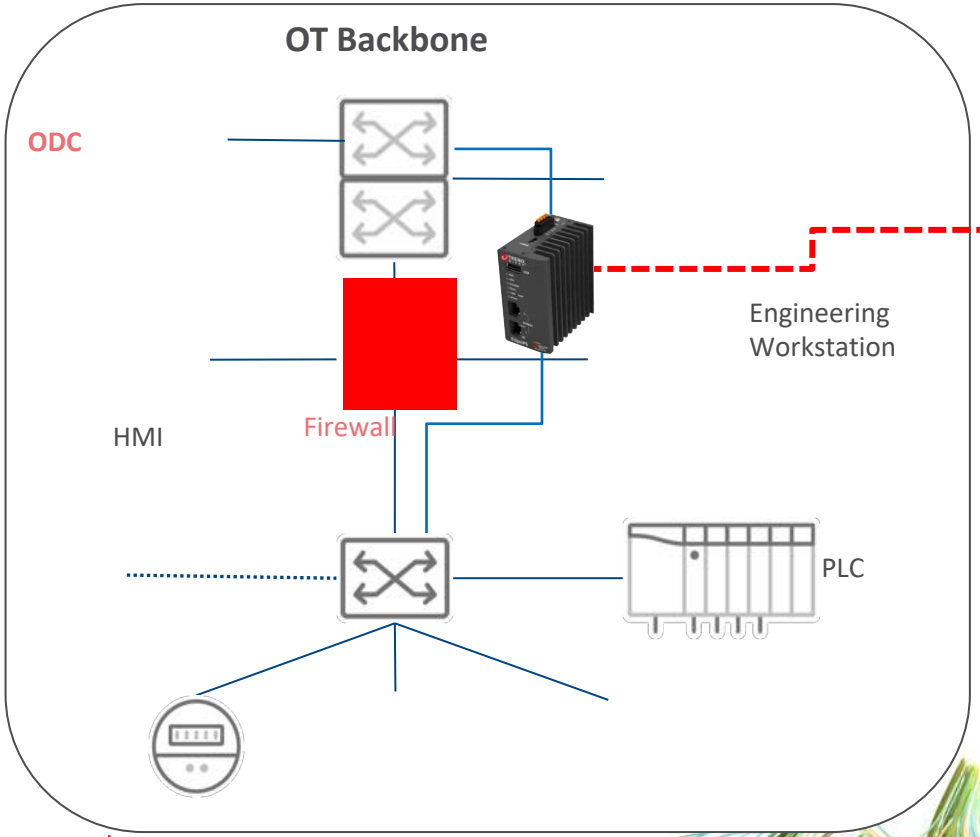
1. 위협 공격을 차단하지 않고 모니터링 / 탐지
2. 위협 공격 이벤트 로그

!"#.(/-/*/0#12,-'0,3-,45

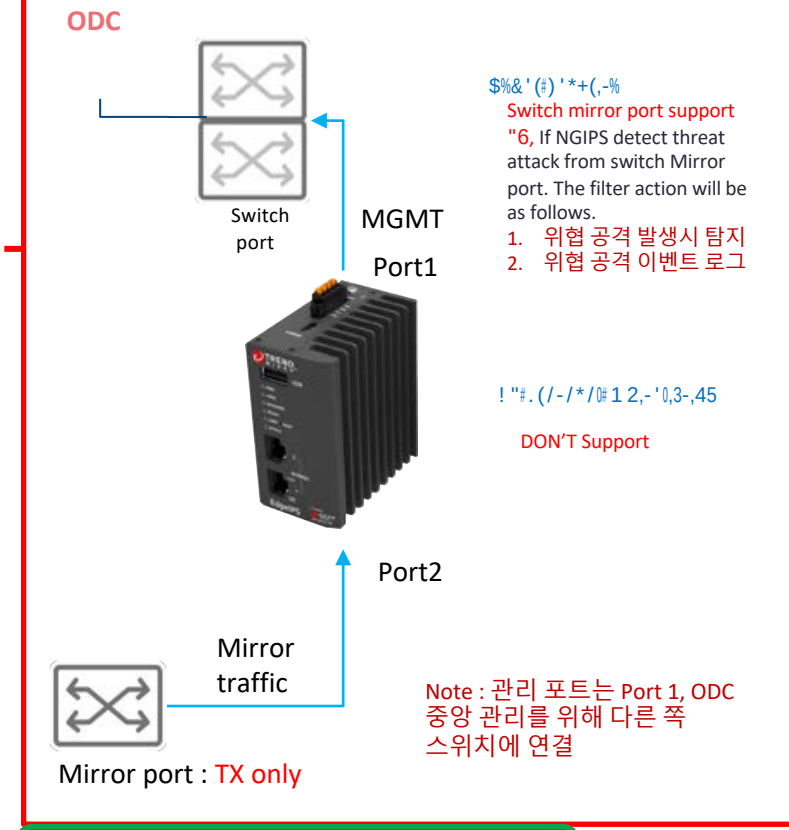
If NGIPS detect malfunction code access and Don't take any action, only detection log , the action will be as follows.

1. 비정상적 OT 프로토콜 접근 탐지, 차단하지 않음
2. 이벤트 로그

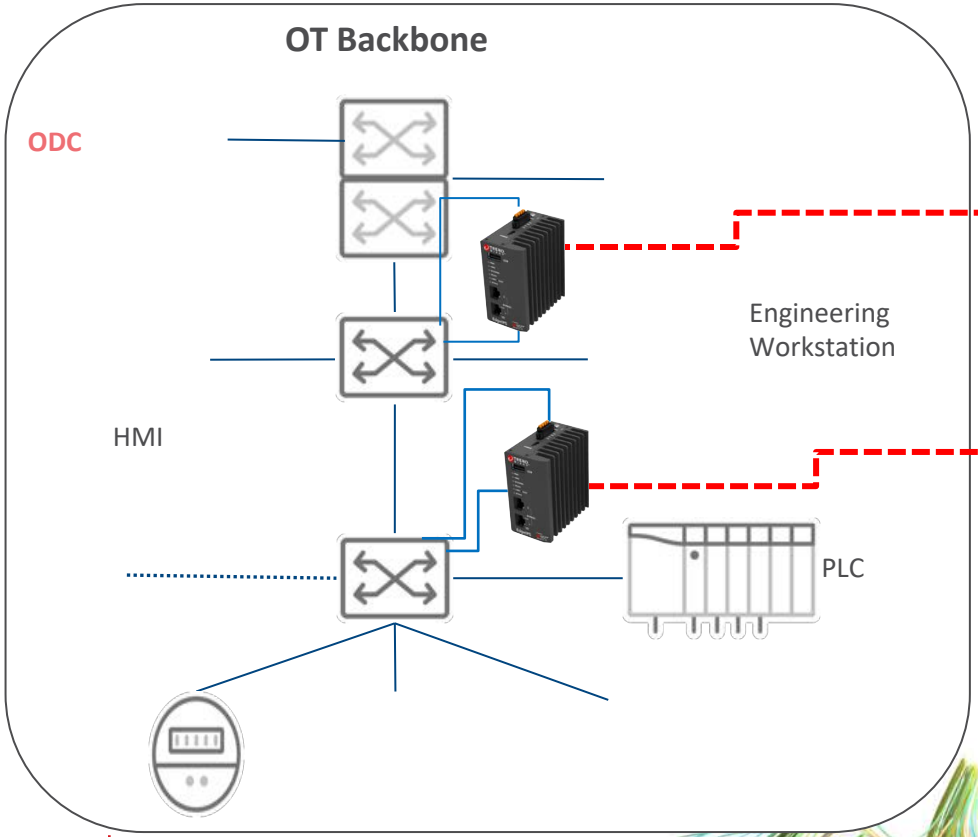
Detection and Monitoring



Offline Monitor mode-1 (Connected with different switch)



Mirroring traffic Detection and Monitoring



Offline Monitor mode-2
(Connected with the same switch)

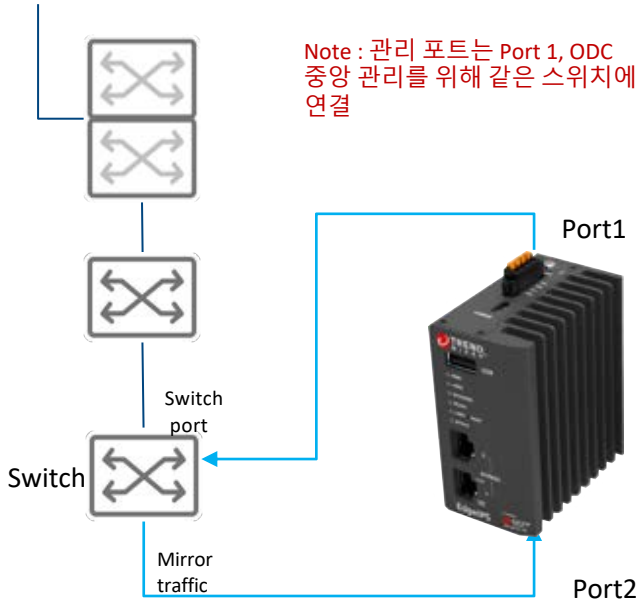
$%&'(#)'*+(,-%

Switch mirror port support "6, If NGIPS detect threat attack from switch Mirror port. The filter action will be as follows.

1. 위협 공격 발생시 탐지
2. 위협 공격 이벤트 로그

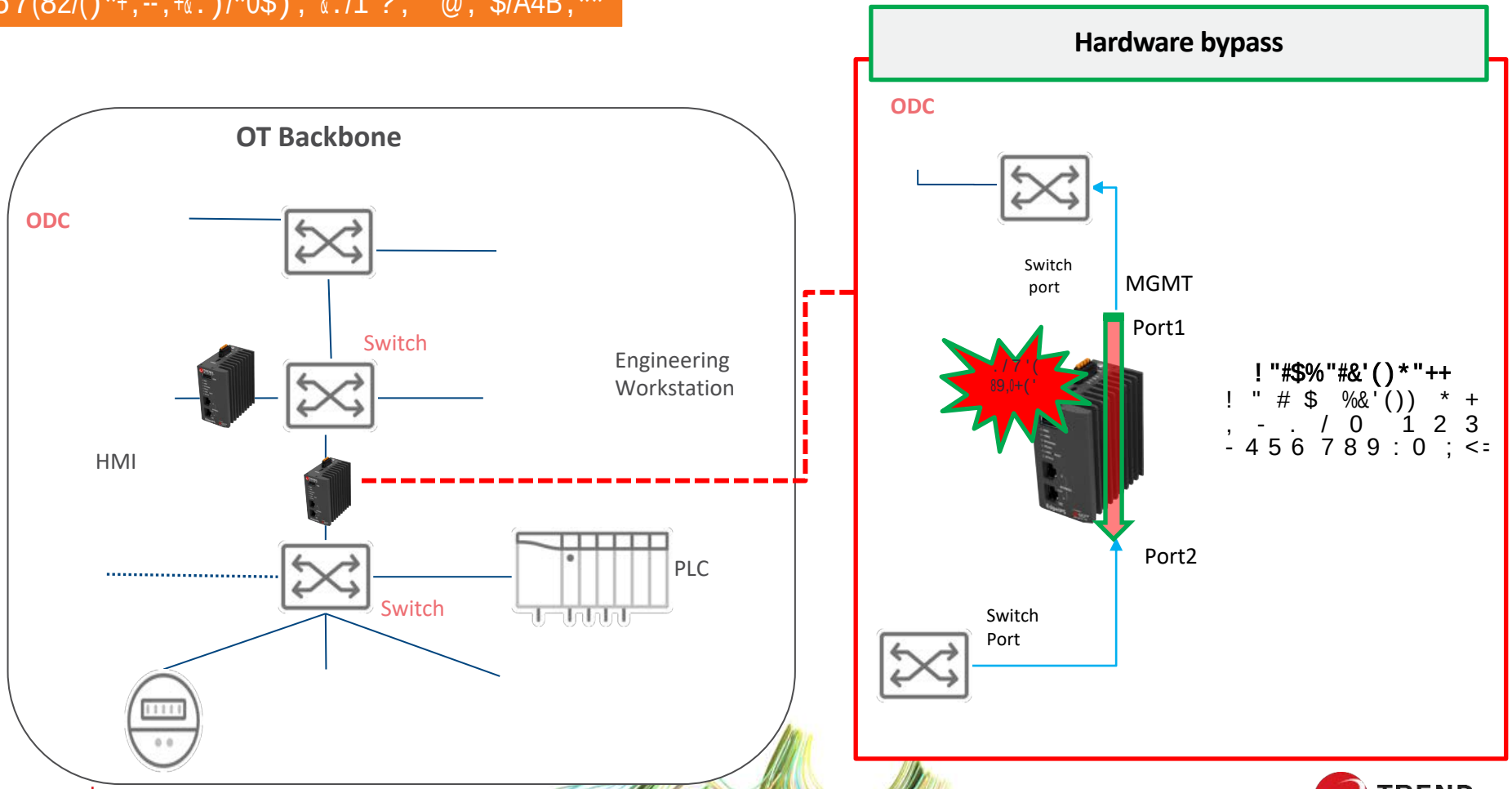
ODC

! "#.(/-/*/0#1 2,-'0,3-,45 DON'T Support

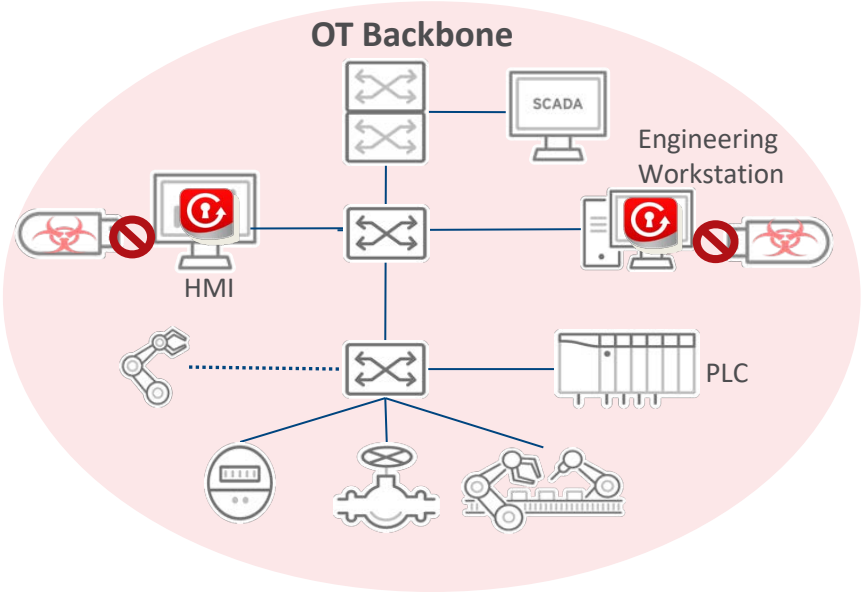


Mirror port : TX only

Mirroring traffic Detection and Monitoring



TxOne SafeLock-ICS



- 실행 파일, 레지스트리, 설정파일등 SafeLock “Lockdown”기능으로 변조 방지 및 무결성 보호
- 보호 시스템에는 반드시 허가된 USB만 허용
- USB 컨텐츠 보안

Trend Micro Portable Security 3

폐쇄망 시스템들을 위한 악성코드 검사 및 치료 툴

설치가 필요 없음

- 백신 설치가 안되는 중요 시스템들을 위한 디자인

간편한 사용

- USB 타입 연결로 악성코드 검사 및 치료
- 내장된 LEDs 디스플레이로 검사 상태 표시

다양한 플랫폼 지원

- 단종된 버전부터 최근 버전의 윈도우 및 리눅스 기반 시스템 지원

허가되지 않은 OT 자산 체크

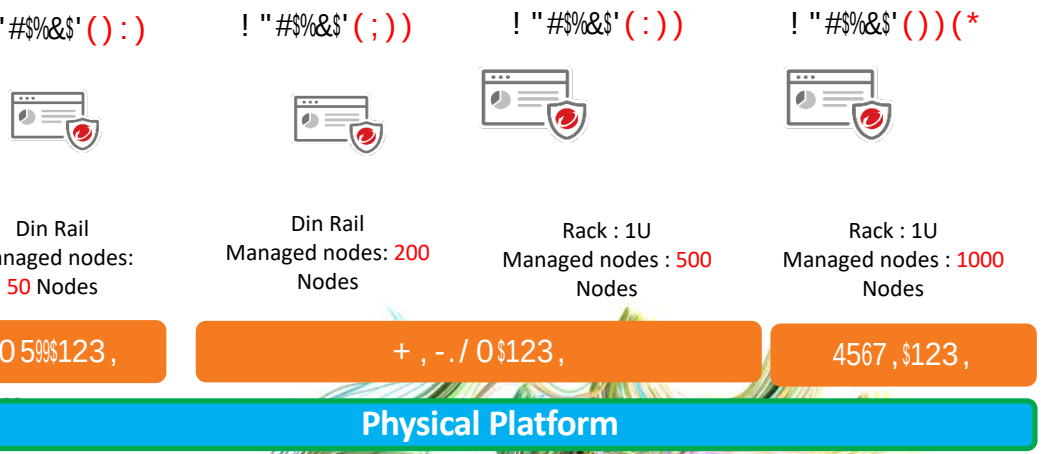
- 검사하는 동안 시스템 정보, OS 업데이트, 어플리케이션 목록 등을 포함한 상세한 자산 정보 수집

중앙 관리

- 패턴 업데이트, 설정 배포, 검사 로그와 자산 정보의 상관관계는 중앙 콘솔로 통합 관리

! "#$%&%'(%#)*'(*+%

- ! !"#
  - ! " # $ % & ' ( ) * + , $ + -
  - . / 0 1, 2 3 4 5 6, 7 8 9 : - ; < = > ?
  - @ A B, 6 C D E F G H I J K L M C N @ O
  - IT SOC(7 8 # >) P OT 7 8 , ; < = F G



OT Defense Console – 주요 기능

대시보드

OT 네트워크 가시성

보안 센서 관리

ODC–
Physical Appliance

그룹별 보안 정책/개체

OT 프로토콜 화이트리스트

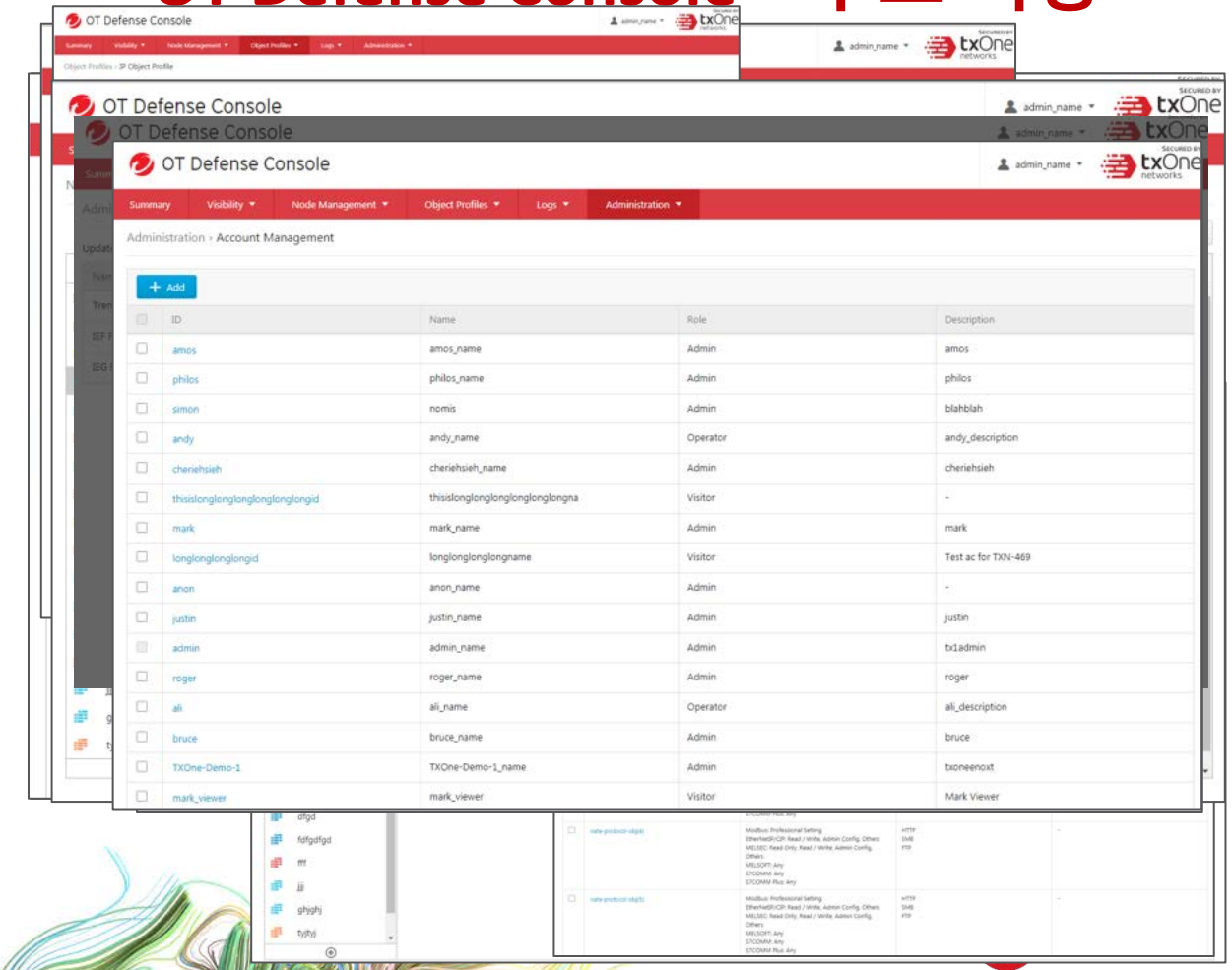
ODC–
Virtual Appliance

IPS/IDS 정책 관리

패턴 업데이트

로그 조회/알람

사용자 관리



Trend Micro TXOne 국내 고객 사례

Deployment

EdgeIPS™

Intrusion Prevention System (IPS)
Protocol Whitelisting

EdgeFire™

Intrusion Prevention System (IPS)
Network Segmentation

Safe Lock™ (TMSL)

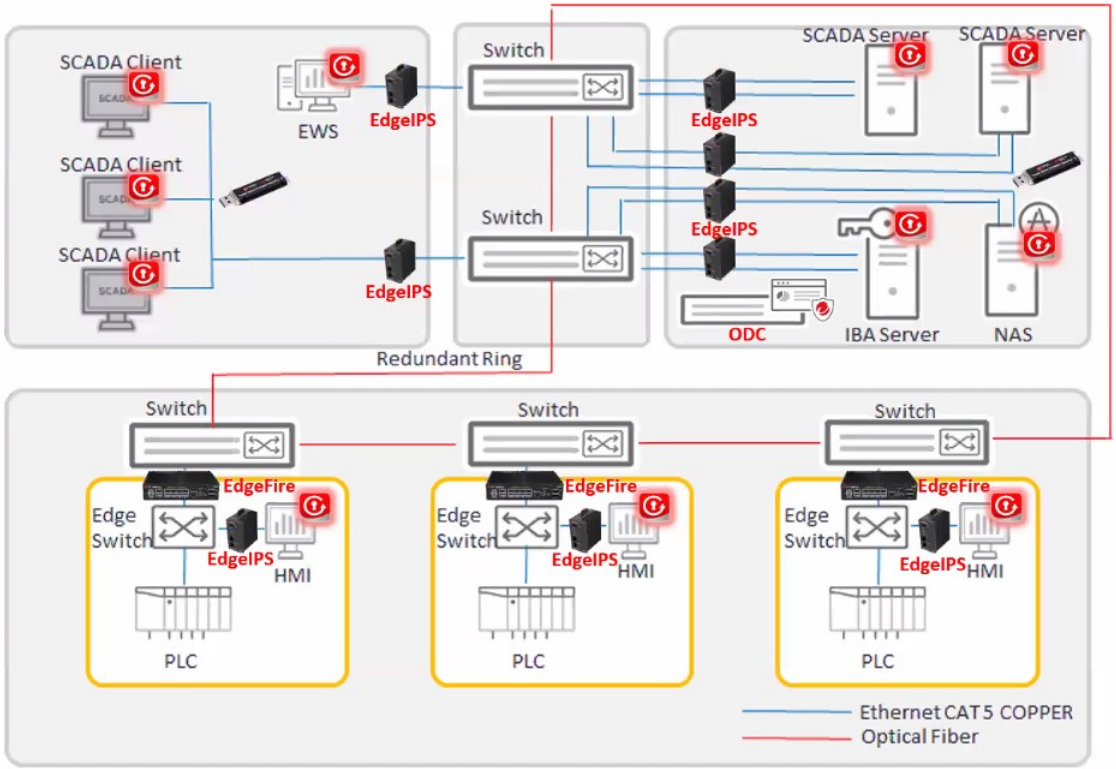
Lockdown AV solution
without using pattern file

OT Defense Console™ (ODC)

Centralized Management
Group Management

Trend Micro Portable Security 3™ (TMPS3)

USB stick AV scanning solution
without installation




Trend Micro
TXOne Solutions