ROVERMOOT
www.rovermoot.co.kr

OT보안! 더 이상 미룰 수 없는 이유

ROVERMOOT

More secure and reliable service provider

2024

OT보안의 필요성 대두

THE SECURE AND RELIABLE PARTNER

DATANET

[2024 보안 전망⑥] 첨단 공격 기술 향연장 된 OT

높은 수익 얻을 수 있는 제조·의료 집중 공격

OT 공격은 사람들의 일상생활과 생명, 재산을 위협하고, 국가안보에도 큰 위기로 다
코로나19 이후 세계 곳곳에서 전쟁이 발생하고 있는데, 현대전은 물리적인 전쟁과
이 결합된 하이브리드전으로 진화하고 있어 더 큰 피해를 일으키고 있다. 더불어 랜
자들이 더 높은 몸값을 얻어내기 위해 OT를 집중적으로 노리고 있으며, 높은 수익을
제조업, 의료기관에서 큰 피해가 발생하고 있다.

가장 많은 공격을 당하는 산업은 제조업으로, 매년 전체 사이버 공격 중 제조업을 대
이 20%를 넘으면서 1위에 오른다. SK쉴더스 조사에 따르면 국내에서 2023년 발생한
공격이 20%로 가장 높은 비중을 차지했다. 전 세계적으로는 전쟁 여파로 공공·정부
한 핵티비즘이 21%였다.

최근에는 병원을 타깃으로 한 공격이 크게 늘어났다. 병원은 첨단 IT 기술을 접목한
비와 민감한 개인 의료정보를 갖고 있어 공격 시 높은 수익을 얻을 수 있다. 그런데 병
은 사이버 보안 대책이 충분하지 않기 때문에 쉽게 공격할 수 있다. 민감한 의료설비
반 IT 보안기술로 보호하기 어려운 경우가 많으며, 상세한 자산관리와 취약점 정보
않다.

OT·사이버 보안·OT 보안 전문성 모두 필요

OT 보안은 OT 환경의 특수성을 이해하면서 보안에 대한 전문성도 갖춰야 하기 때문
가 쉽지 않다. OT가 요구하는 높은 가용성을 지키면서 교묘하고 지능적으로 진행되
까지 차단해야 하기 때문이다.

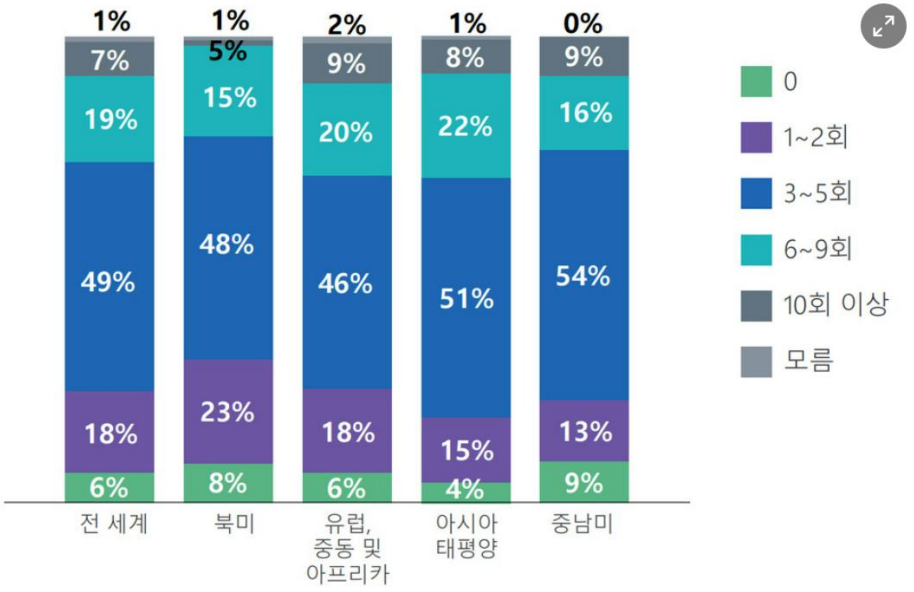
<출처 : 데이터넷(좌) , CCTV뉴스(우)>

CCTV NEWS

[특집기획] 갈수록 복잡해지는 업무 환경, OT 보안의 필요성도 커져

아직은 효율성을 더 추구하는 기업 환경

보안 기업 포티넷이 지난해 말 발행한 '2022년 운영 기술 및 사이버 보안 현황 보고서'에 따르면 기업들의 OT 보안 필요성에 대한 인식은 갈수록 커지는 것으로 나타났다. 500명 이상의 OT 보안 전문가를 대상으로 조사한 내용을 바탕으로 작성된 이 보고서에서 응답자의 94%가 연 1회 이상의 보안 침해를 경험한 것으로 나타났다. 3회 이상의 침해를 경험한 응답자는 74%였으며, 10회 이상의 침해를 경험한 응답자도 7%에 달했다.



2022년 보안 침해 횟수[출처: 포티넷 보고서]

OT보안이란?

THE SECURE AND RELIABLE PARTNER

OT 보안이란?

OT (Operation Technology)는 산업운영기술로 산업제어시스템(Industrial Control System : ICS) 또는 SCADA 뿐만 아니라 일반 네트워크와 함께 연결되어 사용하는 다양한 산업 환경을 의미합니다.

OT 보안은 이러한 산업 환경을 여러 위협에서 방어하는 것을 이야기 합니다.

OT 보안이 필요한 이유?

1 설비 시스템의 Update 및 Patch의 어려움

설비 운영의 중단이 어려운 OT 환경 특성 상, Update 및 Patch, 백신 설치 등에 제약 발생.

2 노후화된 시스템으로 인한 취약점

설비 시스템의 노후화된 OS, Patch의 어려움으로 인한 다수의 취약점이 존재.

3 제조업에 집중되고 있는 OT보안 사고 사례

최근 랜섬웨어 등의 공격은 제조업에 집중되고 있으며, 실제 피해 사례 또한 증가.

4 운영 중단에 따른 막대한 비용 손실

설비 시스템의 감염으로 인한 운영 중단 시, 제조 또는 입/출고 등의 업무 중단 발생.

ROVERMOOT
www.rovermoot.co.kr

OT보안을 위한 OT Defender

THE SECURE AND RELIABLE PARTNER

OT Defender 보안 서비스 개요

OT Defender는 산업용 네트워크 보안 솔루션으로, 산업제어시스템(ICS)에서 사용되는 SCADA, DMI 등의 다양한 Protocol을 지원하며, OT 네트워크 환경에서 네트워크에 대한 필터링과 취약점에 대해 방어할 수 있는 환경을 제공 합니다.

OT Defender 기대 효과

- 산업제어시스템(ICS)에서 사용되는 다양한 Protocol을 포함해 Window 및 Linux 등의 다양한 플랫폼들을 방어할 수 있는 환경 제공.
- IPS(침입차단) 외에도 Bonet, 네트워크 기반의 Anti-Virus 등의 다양한 보안 옵션을 제공.
- 네트워크 구성 변경 없이 간편한 배포 가능.
- 설비들의 네트워크 중단 없이, 보안 기능에 대한 차단/탐지 모드의 전환이 가능.
- Cloud 기반의 중앙관리를 지원. (설치형 중앙 관리 제품 또한 가능)
- 일반적인 유선(Wire) 환경 외에도 Wireless(무선) 전용 제품 지원.
- -40도 ~ 70도 까지의 운영 온도로 다양한 환경에서 안정적으로 동작.

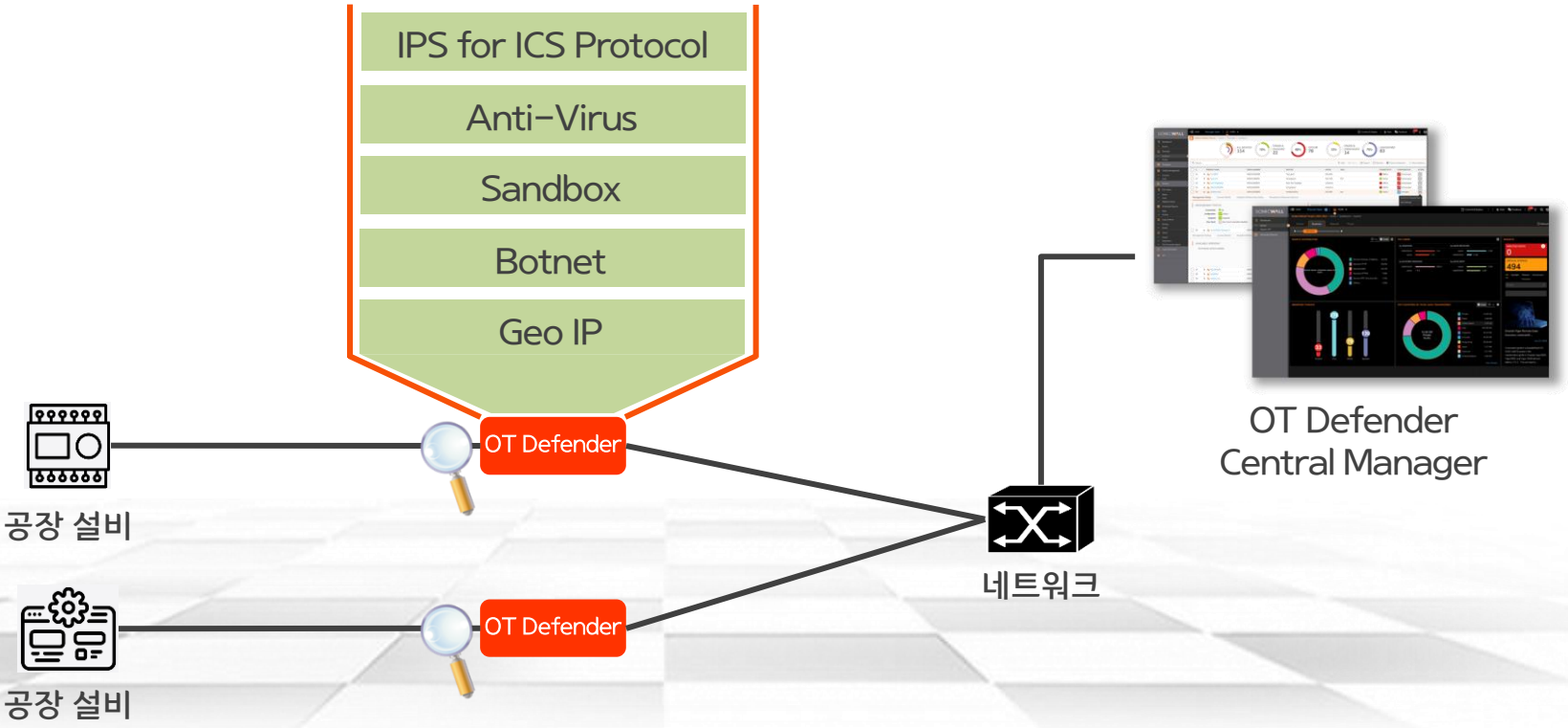
OT보안을 위한 OT Defender

THE SECURE AND RELIABLE PARTNER

OT Defender 동작 방식

OT Defender는 공장의 설비와 네트워크 장비 사이에 위치하여, 설비와 설비 또는 설비와 인터넷 등의 일반 네트워크 간의 통신에 대해 IPS를 포함해 Anti-Virus, Sandbox, Botnet 등의 기능에 대해 탐지/차단 처리 합니다.

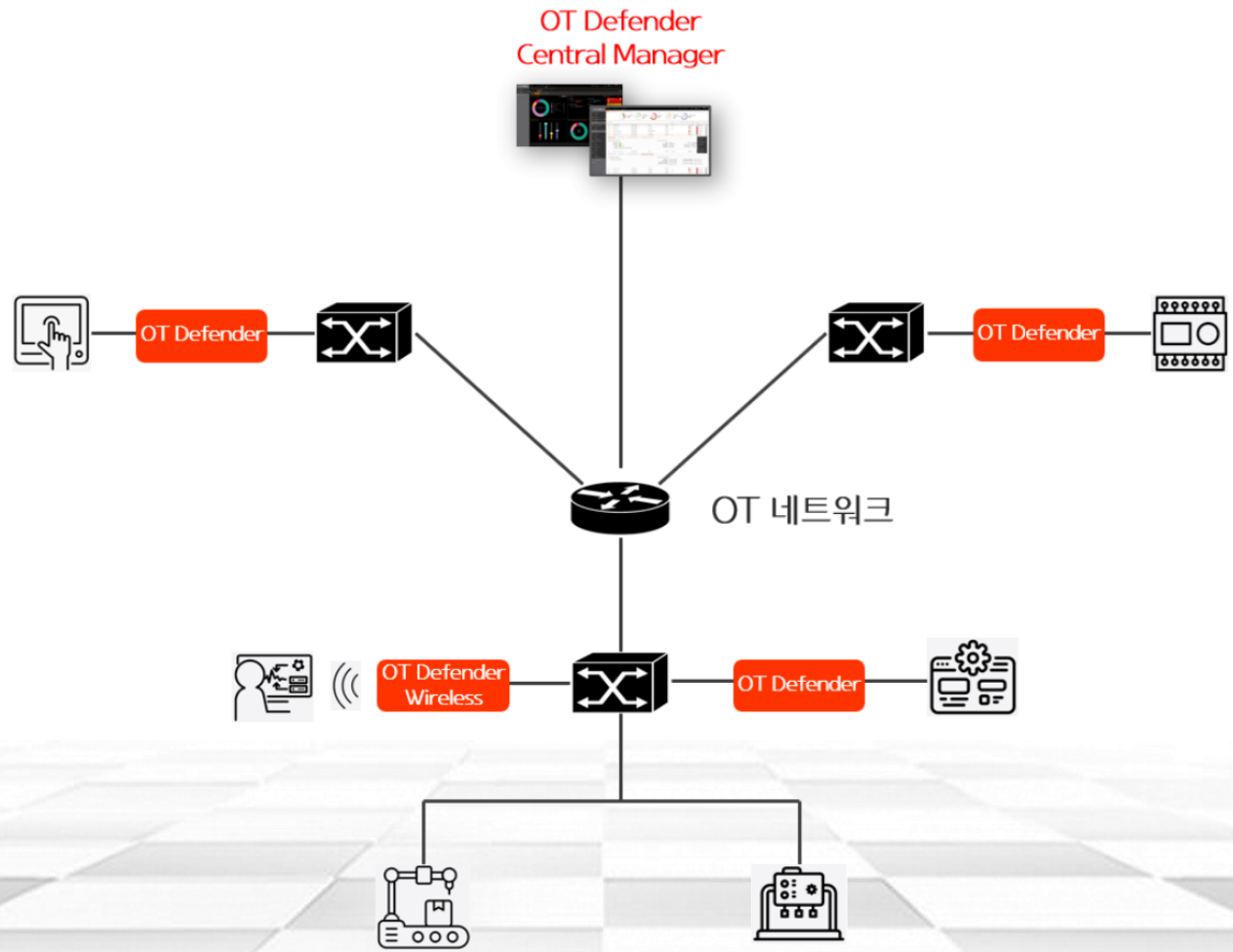
또한, 전용의 Central Manager를 통해 OT Defender는 중앙 관리 됩니다.



OT보안을 위한 OT Defender

THE SECURE AND RELIABLE PARTNER

OT Defender 예시 구성도



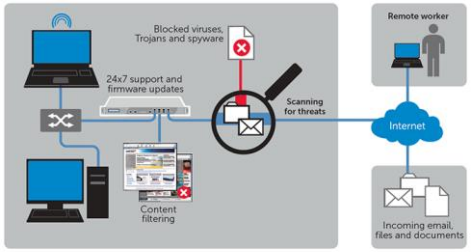
ROVERMOOT
www.rovermoot.co.kr

OT보안을 위한 OT Defender

THE SECURE AND RELIABLE PARTNER

OT Defender 지원 기능 상세

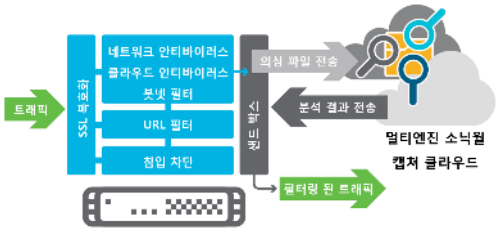
Anti-Virus & IPS



TotalSecure network

- HTTP, FTP, IMAP, SMTP, POP3, CIFS/Netbios, TCP Stream 에 대한 Anti-Virus 지원
- SCADA 및 HMI, CIP 등 다양한 ICS Protocol 지원
- 약 30,000 개의 시그니처 내장
- 약 6,000만개의 Cloud AV 시그니처 제공

Sandbox



- 4개의 멀티엔진의 가상 샌드박스
- Real-Time Deep Memory Inspection
- 하이퍼바이저 레벨 분석
- 풀 에뮬레이션
- Block until verdict

Geo IP, Botnet

- 국가별 IP 정보를 이용하여 특정 국가 접속 차단
- 멀웨어 감염 후 C&C 서버 접속 차단

OT보안이 필요한 이슈

THE SECURE AND RELIABLE PARTNER

OT 보안의 필요성

OT보안은 IT 보안과는 다르게 설비들의 운영이 중단되는 안되는 환경입니다. 즉, OT 환경에서는 설비들의 가용성이 중요시 되고 있습니다.

이러한 중단이 어려운 환경에서 설비들의 운영 체제를 Update 또는 Patch 하거나, 백신 설치와 같이 설비 시스템의 재부팅이 필요한 작업에 제한이 있을 수 밖에 없고, 이 부분은 설비 시스템에 다수의 취약점에 노출되도록 합니다.

최근 OT 보안 사고 사례는 제조업에 집중되고 있으며, 랜섬웨어를 포함해 다양한 방식으로 설비 운영을 중단 시키는 공격이 증가되는 추세인 환경에서 OT Defender를 통해 최소한의 방어 체계를 구현하시기 바랍니다.


THANK YOU