

OT 보안 원격 및 접근 통제를 위한 공장 설비 기계 원격제어 솔루션 소개서

 RemoteView OT



정보보안경영시스템 인증기업 ISO/IEC 27001:2022, 27017:2015

 RSUPPORT

목차

INDEX

I. 제안사 소개

II. 제안 개요

III. 제품 소개

IV. 특징점

V. 기능 소개

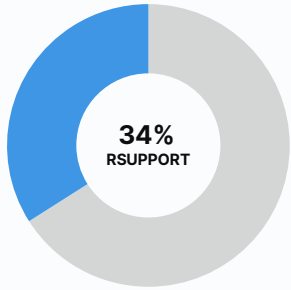
VI. 옵션 소개

VII. 도입 사례

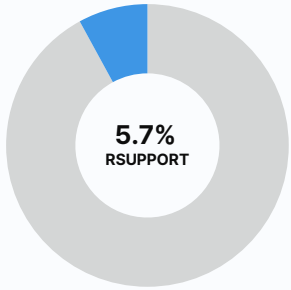
원격 시장을 선도하는 클라우드 서비스 전문 기업

알서포트(주)는 원격지원·제어 솔루션을 개발 및 공급하는 글로벌 기업으로, 설립 이후 지속적인 매출 성장과 수출 실적을 이뤄내며 글로벌 원격지원 및 제어 시장을 선도하고 있습니다. 꾸준한 R&D 투자를 통한 제품 고도화 및 원격 커뮤니케이션·협업 솔루션 등 제품 포트폴리오를 강화하고 있습니다. 다양한 운영체제 및 디바이스 환경을 지원하는 알서포트의 원격 솔루션은 세계 24개국 300,000여 고객들로부터 뛰어난 기술력을 인정받고 있습니다.

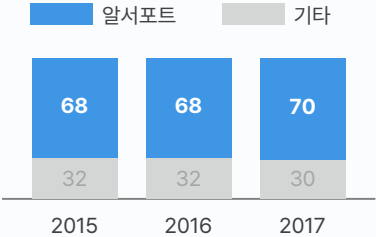
회사명	알서포트 주식회사	설립일	2001년 11월 06일
매출액	504억원 (2023년 12월 기준)	코스닥 상장	2014년 1월 7일 [A131370]
한국본사 및 지사	한 국 : 서울특별시 강동구 고덕비즈밸리로2가길 12 일 본 : 〒105-0001 東京都港区虎ノ門1-2-20 第3虎の門電気ビル 중 국 : 北京市朝阳区阜通东大街6号方恒国际A座2708	임직원	327명 (2026년 5월 초 기준, 해외지사 인원 포함)
		사업영역	소프트웨어 개발 및 공급 (원격지원 및 제어, 협업 솔루션)



아시아 원격 시장 점유율 1위

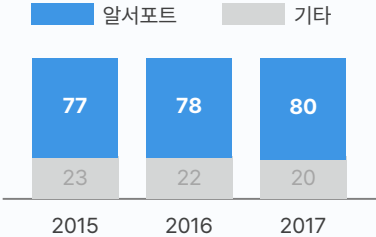


글로벌 원격 시장 점유율 5위



일본 원격 시장 점유율 1위

2015-2017년 일본 원격 시장 M/S 추이
출처 : 일본 경제 연구소



국내 원격 시장 점유율 1위

2015-2017년 한국 원격 시장 M/S 추이
출처 : 한국기업데이터 자료 참고

검증된 품질, 인정받은 기술력

GS 인증, ISO /IEC 획득 등 인증 및 다양한 특허로 당사의 기술력과 안정성을 인증받은 솔루션입니다.

GS 인증

소프트웨어 품질 1등급 인증



ISO/IEC 획득

정보보호 관리국제 표준
(27001:2022,27017:2015)



ISO/IEC 27001:2022,27017:2015

소프트웨어 품질 인증, ISO /IEC 획득

NO	항목	특허 내용
1	특허	터치스크린 이동통신단말기의 원격제어 사용자 인터페이스 방법
2	특허	원격제어 중 이동통신단말기내 정보 접근 차단방법
3	특허	스크린샷을 이용한 이동통신단말기 원격지원방법
4	특허	내부망 연결 관리장치를 이용한 컴퓨터 전원 관리방법
5	특허	원격제어 중 피제어 단말 화면 부분 차단방법
6	특허	원격제어 중 피제어 컴퓨터의 화면신호 차단 장치 및 이를 이용한 원격제어 중 피제어 컴퓨터의 화면신호 차단 방법
7	특허	스크린샷을 이용한 이동통신단말기 원격지원방법

외 100여건 이상의 특허 보유

알서포트 제품 라인업

원격지원 / 제어부터 화상회의 솔루션까지 다양한 제품군을 제공합니다.

OT망 원격 제어 솔루션

리모트뷰 OT

R:RemoteView OT

내·외부 망 간 보안 연결 환경에서, 관리자 통제 아래
제조 현장 설비를 원격으로 안전하게 제어하는 솔루션입니다.

재택근무 솔루션

리모트뷰 SE

R:RemoteView SE

멀리 떨어진 장소에 있는 PC 또는 모바일 장비를 원격으로
제어하여 업무를 처리하거나 기기를 관리하는 원격제어
솔루션입니다.

Helpdesk 솔루션

리모트콜

R:RemoteCall

기업의 상담사가 웹브라우저나 전용 프로그램을 통해 고객의
디바이스에 접속하여, 원격으로 장애를 진단하고 문제 해결을
지원해 주는 원격지원 솔루션입니다.

영상 상담 솔루션

리모트VS

RemoteVS

비대면 금융 거래 시 상담사와 고객의 영상 통화와
안면 인식 기술을 결합하여 실시간으로 본인 여부를 확인하고
신뢰도를 높이는 영상 인증 상담 솔루션입니다.

리모트콜 모바일팩

R:RemoteCall + mobile pack

스마트폰, 태블릿 같은 다양한 모바일 장비의 문제를 신속하게
진단하고 문제 해결을 지원해 주는 모바일 원격지원 솔루션
입니다.

화상 회의 솔루션

리모트미팅

RemoteMeeting

별도 설치 없이 웹 브라우저 접속만으로 회의실을 개설하며
다양한 협업 톨을 지원하여 커뮤니케이션 효율을 향상하는
화상 회의 솔루션입니다.

리모트콜 비주얼팩

R:RemoteCall + visual pack

설명하기 어려운 현장 상황에 고객의 스마트폰을 이용해
실시간으로 중계해 상담사가 신속하게 진단하고 문제 해결을
지원해 주는 영상지원 솔루션입니다.

AI 회의록 솔루션

AI:repoto

Ai:repoto

AI 기술을 바탕으로 화자 구분·인식, 스크립트 기록,
핵심 키워드와 실행 과제 도출 및 요약 등을 자동화하여
업무 생산성을 극대화하는 스마트 회의록 솔루션입니다.

IT·OT 연결 확대로 인한 보안 점점 급증

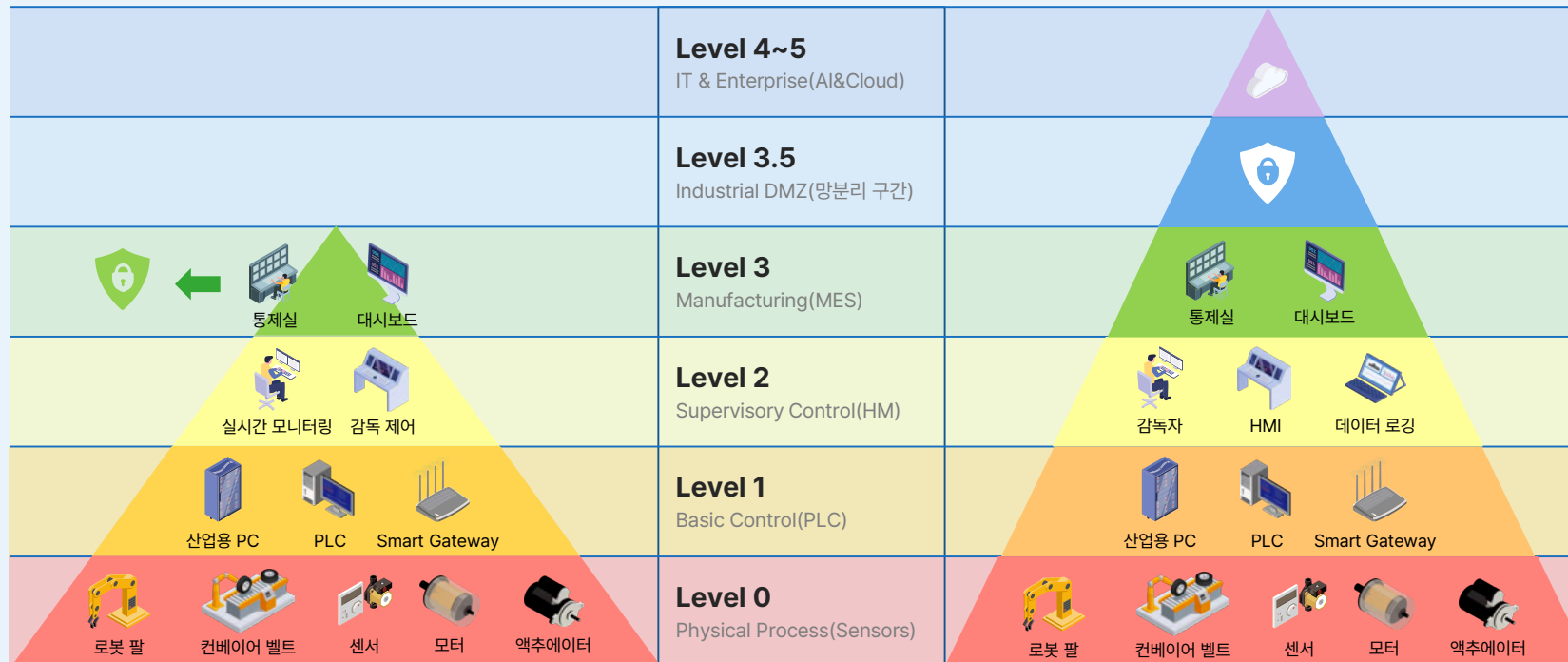
수많은 네트워크 및 S/W 접점이 생겨나며, 모니터링 및 생산 최적화, 예지 보전, 신속한 장애 대응을 하기 위해, 스마트팩토리화 되면서 기존의 폐쇄망에서는 없었던 새로운 보안 사각지대가 발생하고 있습니다.

과거의 OT환경은 폐쇄망으로 외부 위협으로부터 안전했습니다.

현재 IT와 OT의 융합으로 시스템은 혁신적 확장이 되었으나, 그 이면에 보안 위협 또한 급증했습니다.

과거 (AS-IS) 폐쇄망 기반의 물리적으로 안전한 OT 환경

현재 (TO-BE) IT/OT 융합 환경(시스템 확장 및 보안 위협 증가)



핵심 역량 및 인프라

연결 및 네트워크

산업용 이더넷, 5G, Wi-Fi, TSN(시간 민감형 네트워크)

데이터 분석 및 AI

클라우드 컴퓨팅, 빅 데이터, AI 예측 보전

디지털 트윈

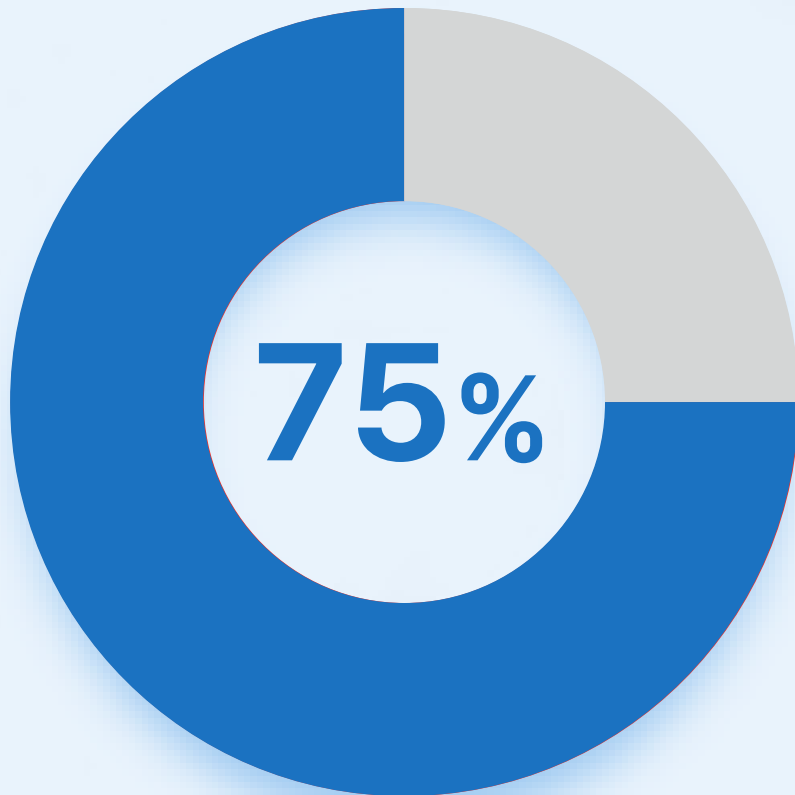
물리적 객체나 시스템을 가상으로 재현

사이버 보안

OT/IT 보안, 방화벽, 접근제어

안전한 OT환경, IT영역의 보안에서 시작

디지털 전환으로 IT와 OT 망의 연결성이 확대됨에 따라, 접점을 안전하게 보호하고 선제적으로 대응하는 통합 보안 관리가 더욱 중요해졌습니다.



**OT 공격의 약 75%는
IT 영역에서 시작되어 OT로 확산됩니다.**



공격자는 자격 증명(Credential)을 탈취하여
정상적인 원격 접속 경로를 통해 침투합니다.



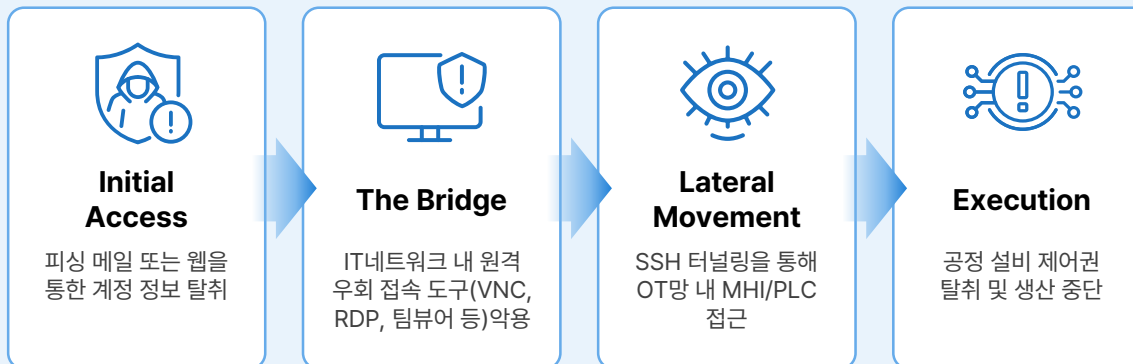
랜섬웨어 그룹의 산업 제어 시스템(ICS) 공격
전년 대비 60% 급증

IT-OT 접점 확대로 인한 보안 리스크 증가

IT 영역과 OT 영역이 융합되고, 무분별한 원격접속은 실제 사고로 이어졌으며 생산 공정 정보, 기밀정보 유출이 발생하고 있습니다. 그로 인해 주요 공정 데이터 유출 및 운영 중단 등의 실질적인 피해를 유발할 수 있습니다.

IT와 OT 인프라가 융합되면서 시스템 복잡성과 보안 리스크가 함께 증가하고 있습니다.

"2026년, 사이버 범죄의 주 타겟은 ICS/OT가 될 것이며, 주 원인은 불안정한 원격접속입니다." (source : Google Cloud Cybersecurity Forecast 2026)



- 관리자 권한 탈취 : 유출된 IT 계정이 OT망 접근의 주요 경로로 악용될 위험성
- Shadow IT : 비인가 원격 제어 도구 사용 등으로 인한 보안 사각지대 발생

OT Security

= 가용성 및 안전 중심 -> 물리적 파괴



물리적 손상

설비파괴 및 오작동 유도



인명 피해

폭발 사고 또는 유해 물질 누출



환경 재해

오폐수 방류 및 오염

보안 취약성 및 외부 공격 노출

외부 공격 노출과 인증 체계의 허점부터 성능 저하 및 관리 사각지대까지의 구조적 한계가 존재합니다.

주요 검토 요건

보안 요소

- 데이터 암호화 여부
- 로컬 디바이스 통제
- 2차 인증 제공 여부
- 접근 제어(IP, Port 등)

관리 요소

- 사용자/관리자 인터페이스
- 장애 복구
- 감사 및 로깅
- 가용성

운영 요소

- 원격 접속 용이성
- 업무 효율성(편의성, 체감속도 등)
- 멀티 플랫폼 지원
- 처리 속도, 다중 접속 제어

오픈소스 원격 제품 취약 위험

인바운드 포트 노출의 위험성

3389/5900 포트 직접 개방은 필수이며, 번호 변경 우회는 수 초 내 포트 스캔으로 무력화됩니다.

다단계 인증(MFA) 부재

단일 암호에만 의존하여 계정 탈취 시 내부망 전체가 장악되는 수평 이동 공격에 매우 취약합니다.

작업 가시성 및 감사 기록 미흡

상세 로그나 전체 세션 녹화 기능이 없어 침입자의 내부 행위 확인 및 사후 원인 파악이 불가능합니다.

랜섬웨어 및 기밀 데이터 유출 통로

PC 1대 감염이 잦산망 전체로 확산되며 실제 12GB 분장의 설계도면이 다크웹에 유출된 사례가 있습니다.

윈도우 RDP/오픈소스 VNC



포트 개방 필수
(3389, 5900)



ID/PW
단순 인증



개별 접속,
이력 관리 미흡

알서포트 RemoteView OT



포트 개방 없음
(보안 게이트웨이)



MFA(OTP, 이메일 등) 필수 적용



중앙 통제 및
전 세션 녹화

알서포트 RemoteView OT 보안 강화



포트 개방 없는 보안 게이트웨이 방식

외부 노출 없이 자체 게이트웨이를 경유하여 해커의 진입점을 원천 차단합니다.

구형 OS 및 특수 장비 에이전트리스 연결

보안 패치가 중단된 장비도 RemoteView BOX를 통해 소프트웨어 설치없이 연결합니다.

연결 방식 : 포트 개방 없음(게이트웨이)

인증 보안 : 다단계 인증(MFA/OTP)

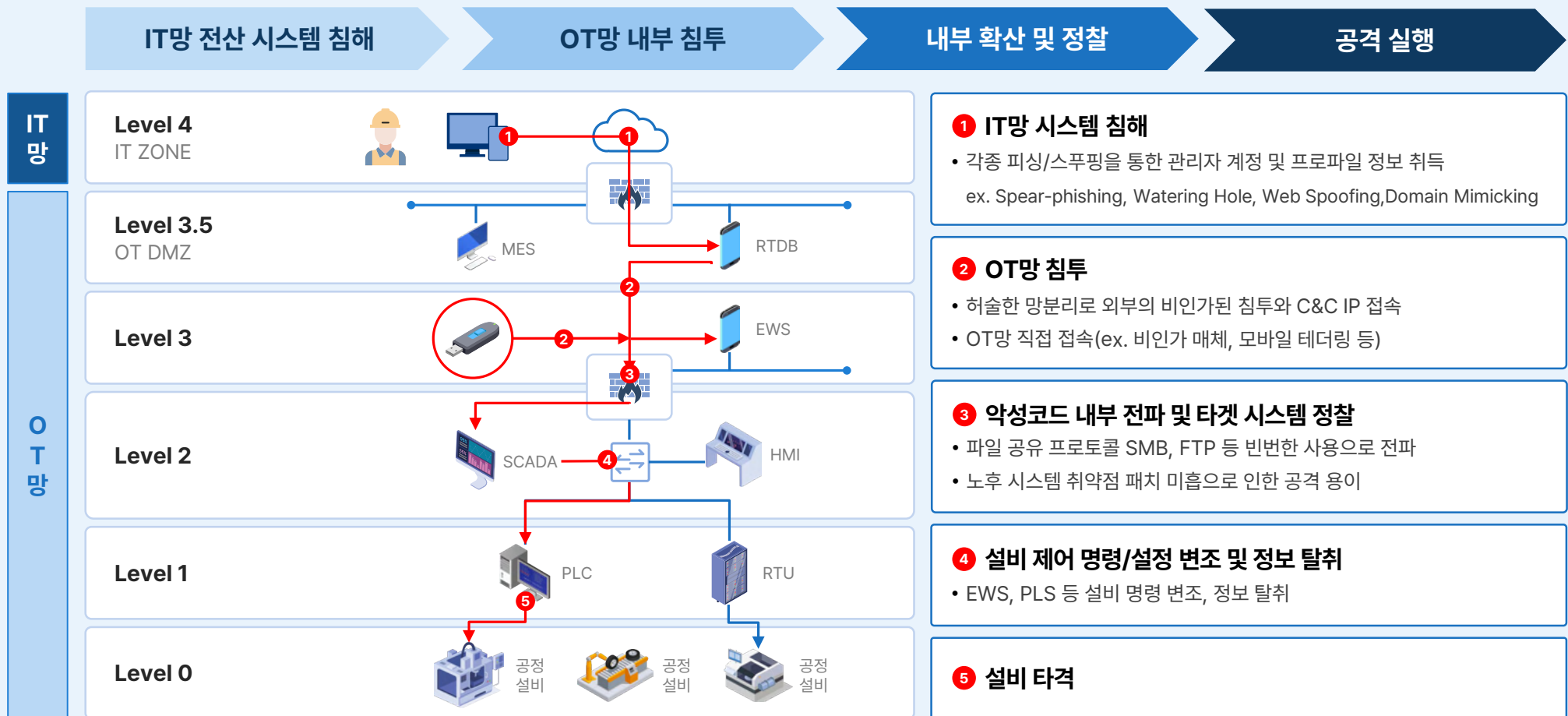
장비 지원 : 하드웨어 방식 전 기종 지원

모 세션 실시간 녹화 및 감사 기능

모든 원격 접속을 영상으로 기록하여 장애 발생 시 원인 추적 시간을 80% 단축합니다.

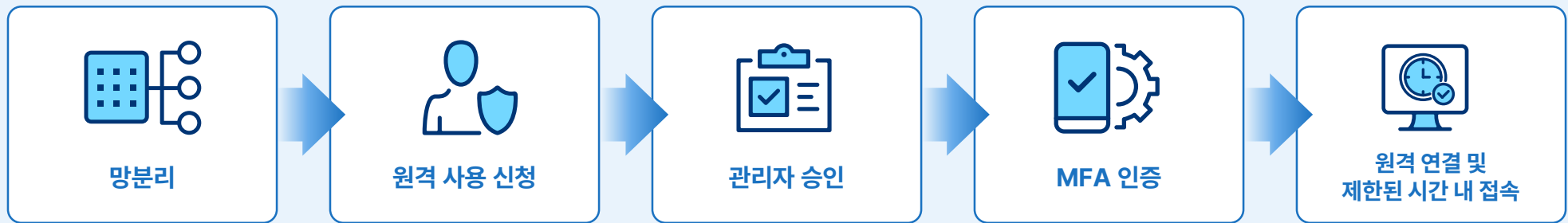
OT 환경하에서 사이버 공격의 전개 양상

사이버 공격 전개는 가장 취약한 영역인 IT 네트워크에서 침해가 발생하여, OT망 내부로 악성 코드가 침입하고, 침입한 악성코드가 공격 대상을 찾아 공격 실행으로 진행됩니다.



스마트 제조 혁신을 위한 OT 보안 원격 제어 전략

안전하게 원격 운영을 하기 위해서 레거시 설비 보호와 보안성, 사용자 통제를 동시에 확보가 가능합니다.



구축 방식

현재 OT 상황 단독 구성 및 외부 통신

OT 최적화 망분리 구성 및 운영

→ DMZ 와 OT망 네트워크 분리 → 외부 통신 차단

접근 방식

현재 OT 상황 VPN 상시연결

OT 최적화 관리자 승인 후 권한 부여

→ 작업 목적/시간에 따른 한시적 권한 부여 → 관리자의 실시간 접속 승인 워크플로우

인증 수준

현재 OT 상황 단일 ID/PW (취약점)

OT 최적화 MFA 및 OTP, 사용자 통제

→ 계정 유출 시에도 추가 인증으로 방어 → 사전 등록된 IP/MAC 주소 기기만 허용

작업 감사

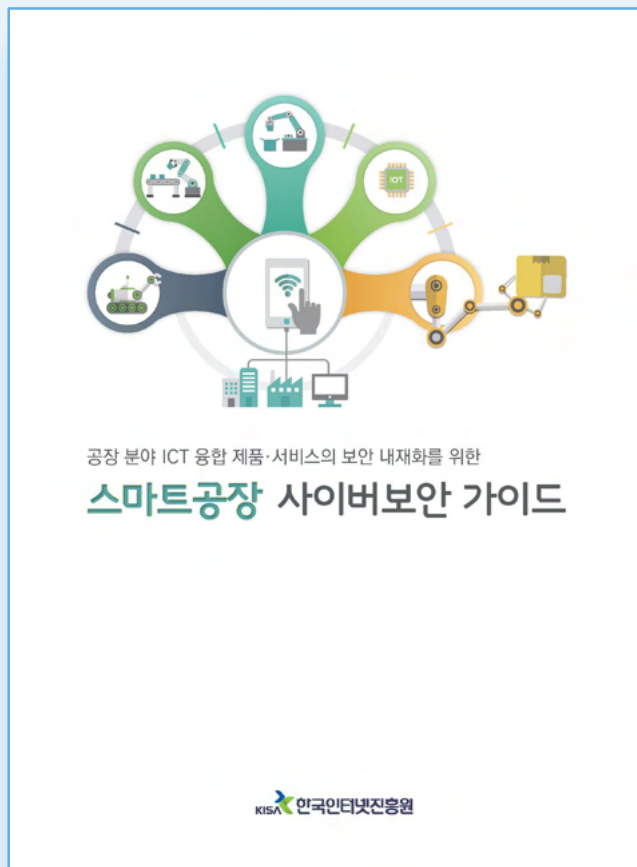
현재 OT 상황 텍스트 로그 위주 (부족함)

OT 최적화 전수 화면 녹화 및 가시성

→ 모든 행위에 대한 이력 적재 → 원격 연결 시 전수 녹화 보관

KISA 스마트팩토리 사이버 보안 가이드라인 준수사항

안전한 스마트팩토리 운영을 위해 KISA(한국인터넷진흥원)에서는 스마트공장 사이버보안 가이드를 제시하고 있습니다.



1

접근 통제

원격접속 확인/프로토콜 검토

스마트공장 내 권한 분리 및 접근제어를 통해 비인가 접근 및 불법접근으로부터 보호해야 한다.

2

데이터 보호

암호화통신/로그 관리/유출 방지

스마트공장 내 다양한 데이터를 보호하기 위해 안전한 저장 정책을 마련하여 접근, 열람, 변조 등을 통제해야 한다.

3

비인가 프로그램 실행 차단

보안 통제 적용

인가되지 않은 프로그램 실행을 차단해야 하며, 시스템 정상 동작 여부를 확인하여야 한다.

4

정보보안 운영 정책 및 절차

사용자 권한 부여

필수적인 사항에 대한 보안 정책 및 운영 절차 수립, 내·외부 직원 관리를 통해 안정적인 스마트공장을 운영하여야 한다.

5

보안 정책 수립

원격접속 솔루션 설치

보안 사고에 대한 신속하고 효율적인 처리 및 피해 복구를 위하여 공장내 시스템의 현황을 모니터링 해야한다.

제품 소개

RemoteView OT 소개

KISA 보안가이드 라인을 충족하는 제품으로써 사용자 PC(Viewer)에서 기업의 사용 설비 PC(Agent)에 원격으로 접속하여 실시간 제어 / 관리하는 원격제어 소프트웨어입니다.

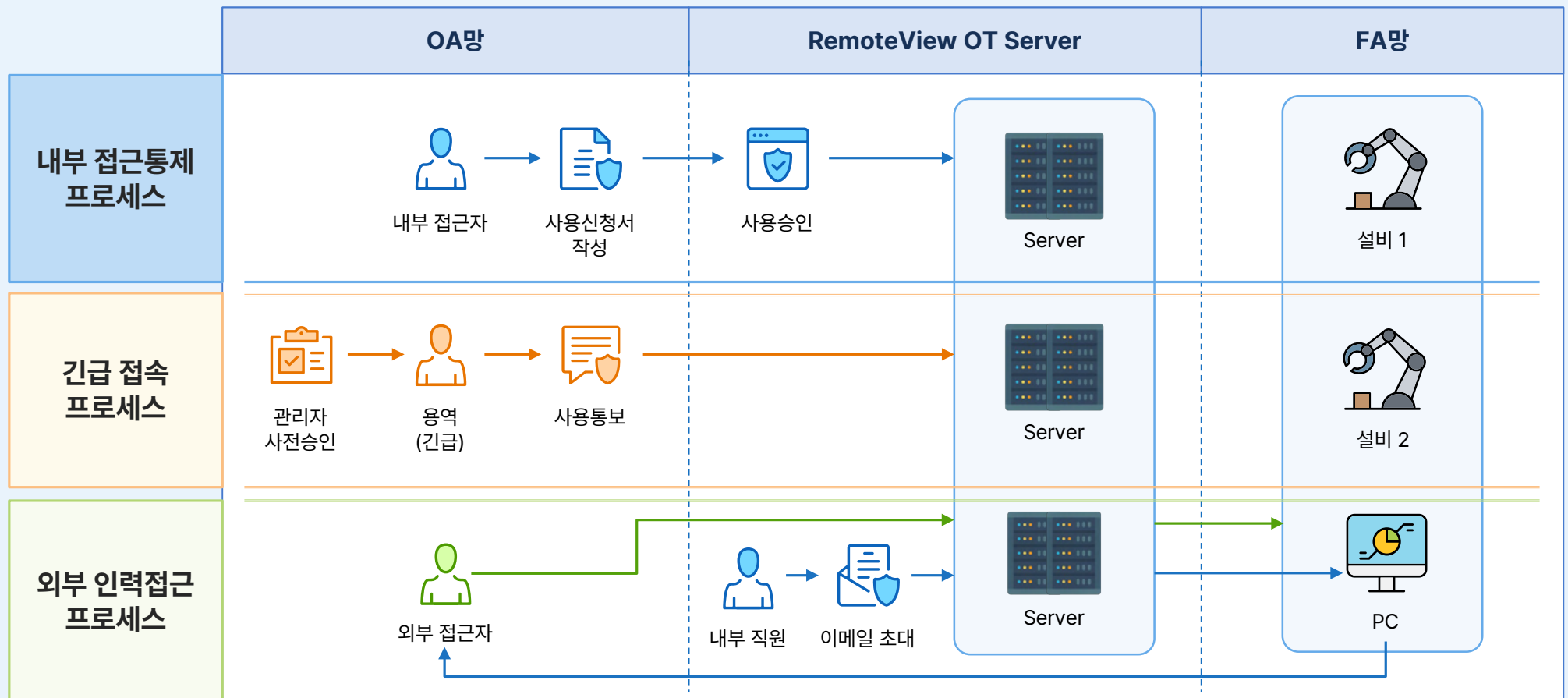


RemoteView OT를 통한 가이드라인을 준수한 안전 원격제어 방법

- 파일 송수신 무결성 검사
- 사용자의 접속 권한 및 이력 관리
- 불필요한 프로세스 접근 차단
- 원격프로그램 단일화하여 중앙관리
- 비인가 사용자 접근 차단

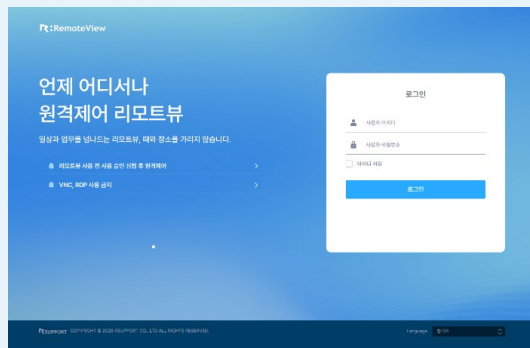
RemoteView OT 접속 프로세스

사용 용도에 맞게 접속 프로세스를 설정하여 운영합니다.

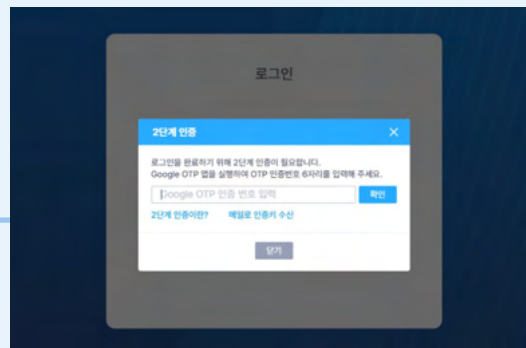


내부 접근통제 프로세스

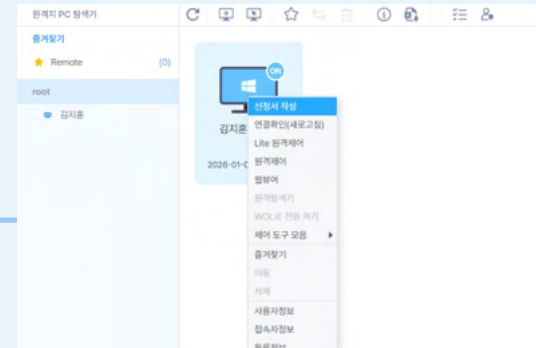
1 발급된 계정을 통해 리모트뷰 로그인



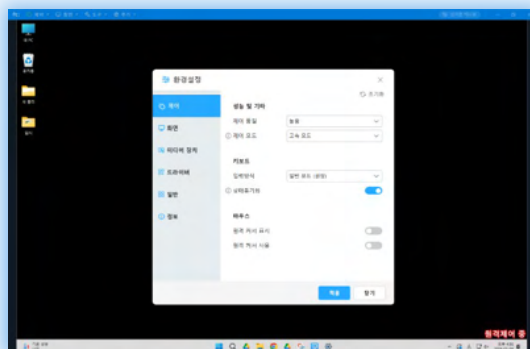
2 OTP를 통한 2단계 인증(선택)



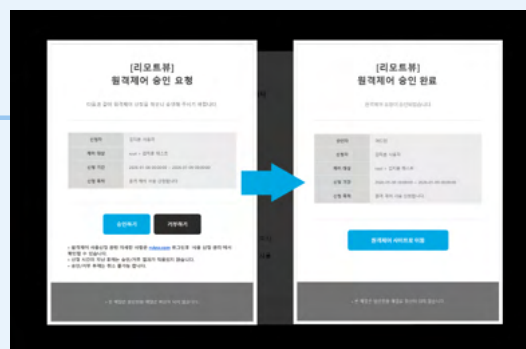
3 원격제어 대상 신청서 작성



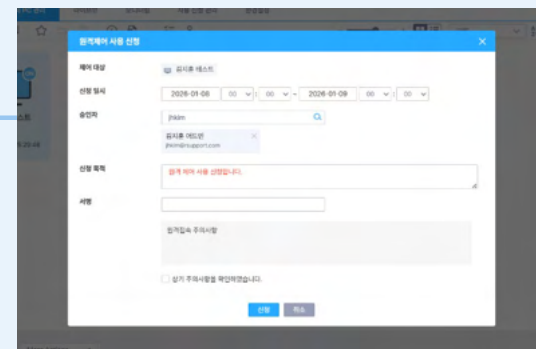
6 원격제어 실행 및 제어

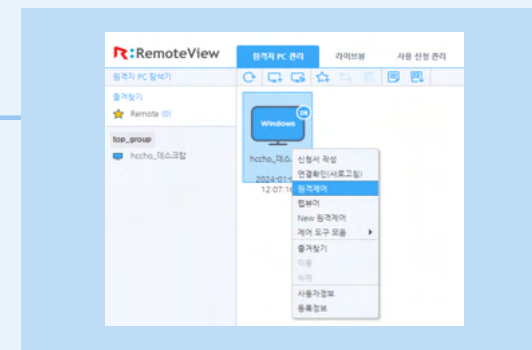


5 신청서 승인 및 승인 완료



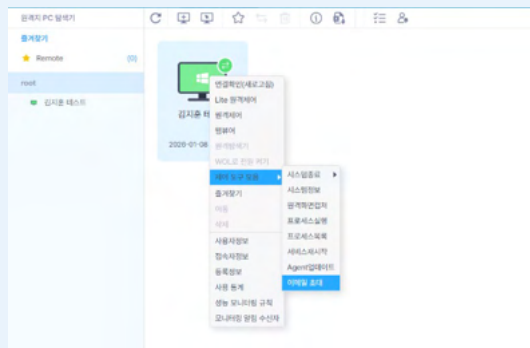
4 신청서 작성 및 서명



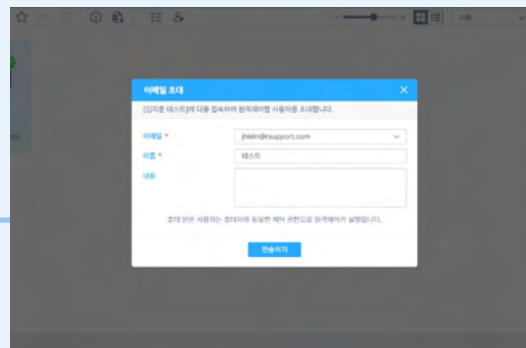


외부 인력접근 프로세스

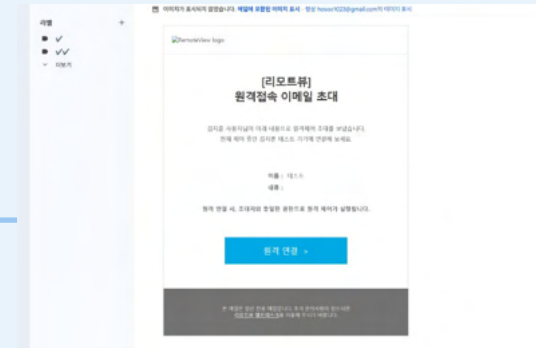
1 내부 승인된 사용자가 원격제어 초대



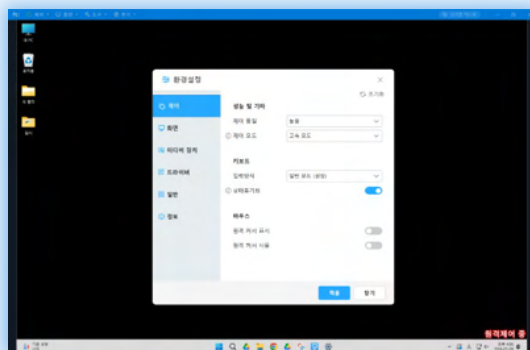
2 외부인력 이메일 발송



3 외부인력 이메일 수신



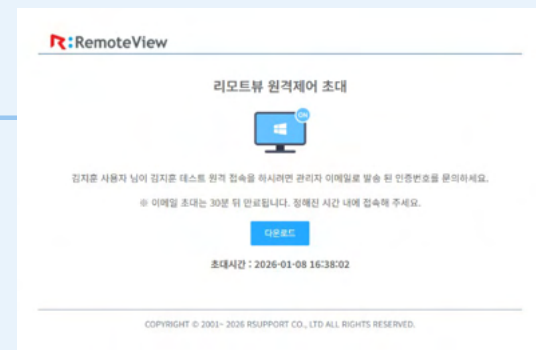
6 원격제어 실행 및 제어



5 내부 임직원이 알려주는 접속번호 6자리 입력 후 실행



4 메일을 통해 원격 초대 확인



듀얼 엔진 시스템

전 구간 암호화 통신

성능 모니터링

멀티 모니터 지원

다중 접속 기능

AI 보고서 및 모니터링

듀얼 엔진 시스템

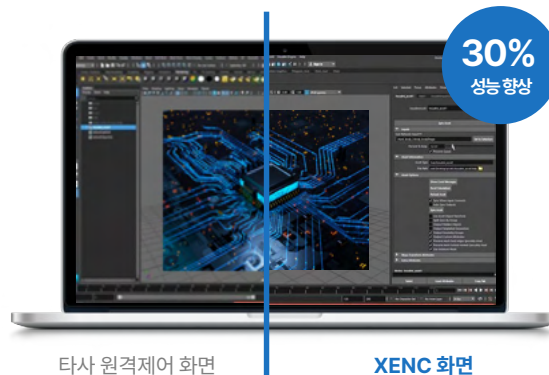
RemoteView OT는 서로 다른 설비 환경을 고려하여 제어 모드를 선택적으로 제공함으로써 운영 안정성과 품질을 동시에 확보합니다.



Lite 원격제어

저사양 PC 및 레거시 장비 지원 최적화

노후 설비·산업용 PC(IPC)·현장 모니터링 장비에 적합, Windows XP SP3~7 지원



원격제어

고성능 인코딩 기반의 선명한 화질 제공

고해상도 화면·세밀한 UI·그래픽 식별이 필요한 환경에 적합, Windows 10 이상 지원

듀얼 엔진 시스템

전 구간 암호화 통신

성능 모니터링

멀티 모니터 지원

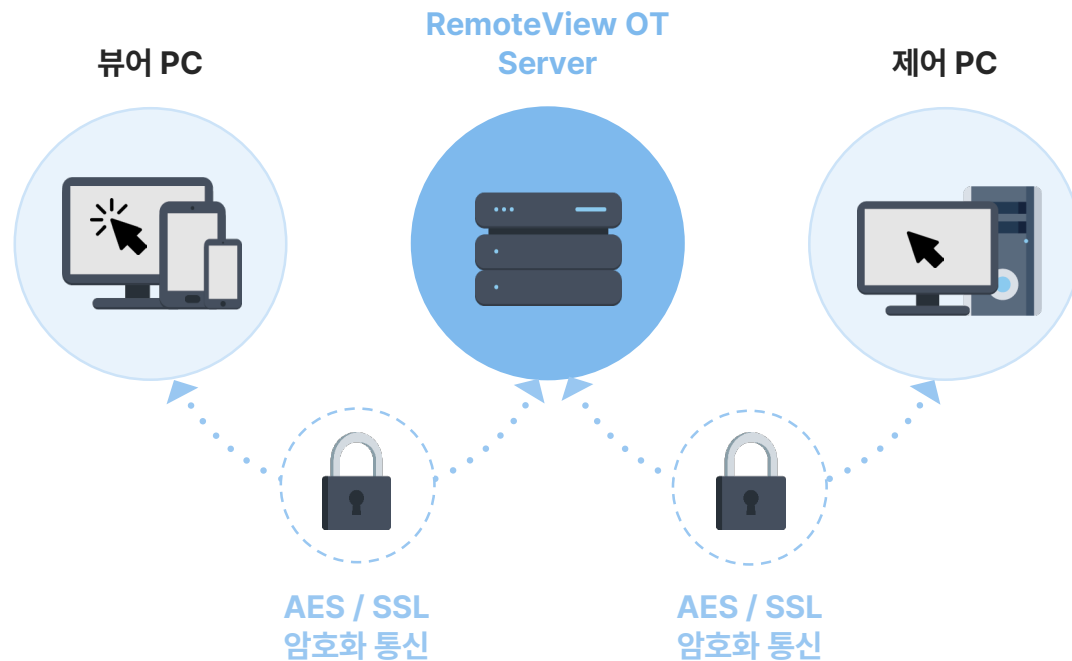
다중 접속 기능

AI 보고서 및 모니터링

전 구간 암호화 통신

RemoteView OT는 전 구간 암호화 통신(AES/SSL 256bit)을 지원하여 보안과 안정성 모두 뛰어납니다.

전 구간 AES/SSL 암호화 통신



듀얼 엔진 시스템

전 구간 암호화 통신

성능 모니터링

멀티 모니터 지원

다중 접속 기능

AI 보고서 및 모니터링

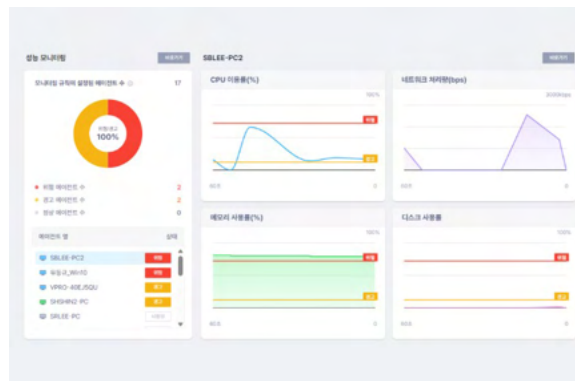
에이전트 PC 성능 모니터링

관리자는 각 에이전트별 CPU 및 디스크, 메모리 등 임계치를 설정하여 모니터링 할 수 있습니다.



성능 모니터링

- 개별 PC의 자원 사용 현황(CPU, 메모리, 디스크)에 임계치를 설정



성능 모니터링 대시보드

- 개별 PC의 자원 사용 현황(CPU, 메모리, 디스크, 네트워크 등) 분석해 성능 저하, 장애 징후, 비정상 행위 등을 미리 파악

듀얼 엔진 시스템

전 구간 암호화 통신

성능 모니터링

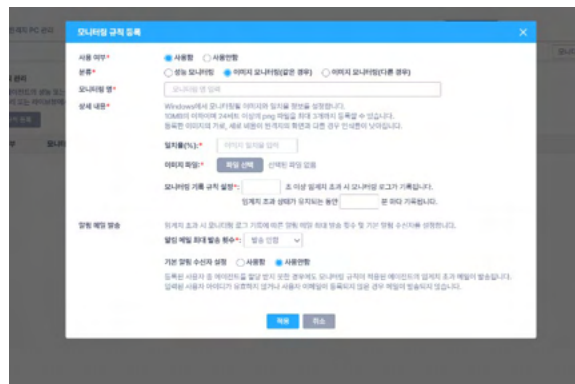
멀티 모니터 지원

다중 접속 기능

AI 보고서 및 모니터링

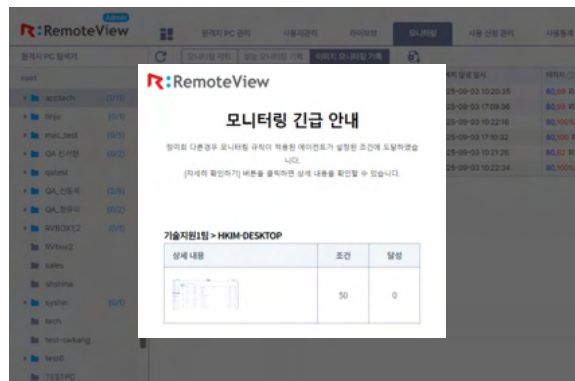
에이전트 PC 성능 모니터링

관리자는 각 에이전트별 CPU 및 디스크, 메모리 등 임계치를 설정하여 모니터링 할 수 있습니다.



이미지 모니터링

- 설비 PC에 변화되거나 변화되면 안되는 경우를 모니터링 하기 위해 이미지를 등록하여 해당 이미지 노출 시 알림보낼 수 있도록 설정



모니터링 팝업 화면

- 원격지 PC 화면을 등록한 이미지와 자동 비교하여 이상 여부를 감지하는 이미지 모니터링 기능을 제공

듀얼 엔진 시스템

전 구간 암호화 통신

성능 모니터링

멀티 모니터 지원

다중 접속 기능

AI 보고서 및 모니터링

멀티 모니터 지원

원격 근무자가 멀티 모니터 사용 시 그대로의 환경을 가져와 똑같은 업무 환경을 조성합니다.

타사 제품



전체보기 또는 단일 모니터 보기 선택

멀티 모니터 지원 안함

모니터 전환 단축키 지원 안함.

RemoteView OT



원격지 PC의 해상도를 뷰어 PC 해상도로 변경

원격지 PC의 모든 화면을 그대로 활용

단축키를 통한 손쉬운 화면 전환

듀얼 엔진 시스템

전 구간 암호화 통신

성능 모니터링

멀티 모니터 지원

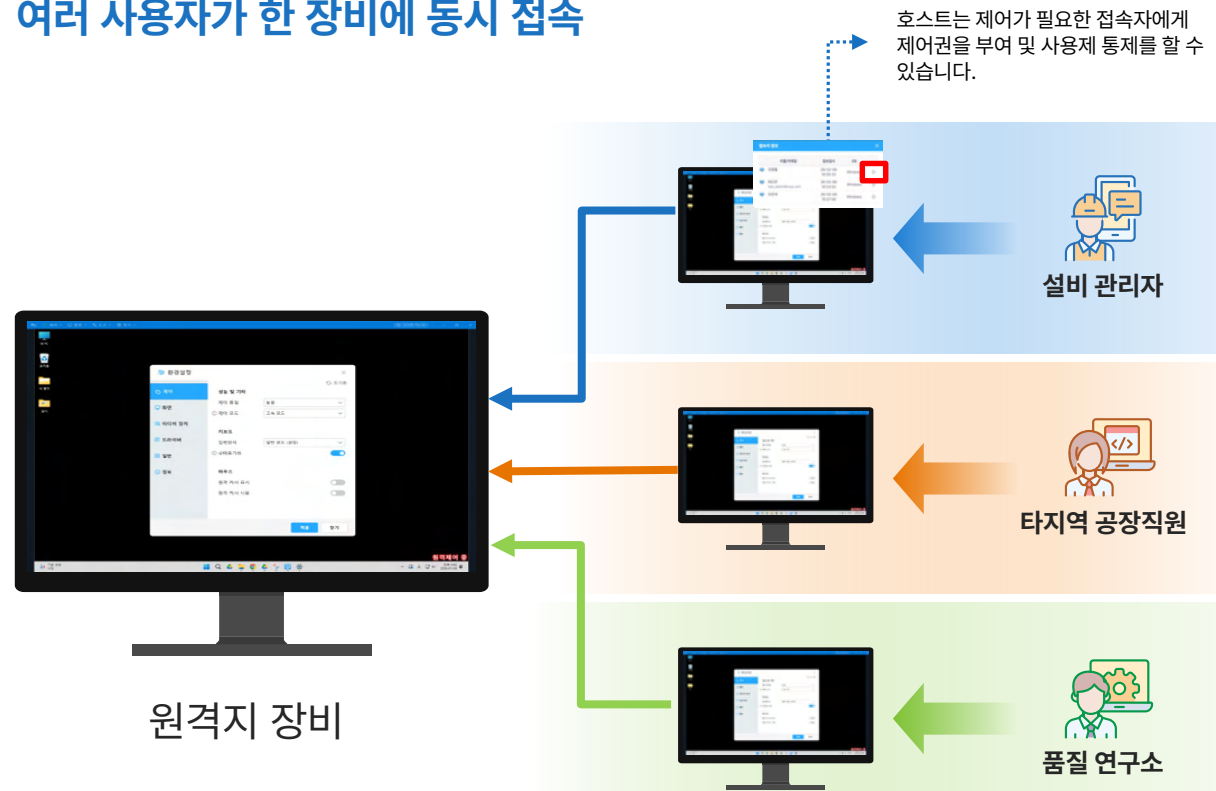
다중 접속 기능

AI 보고서 및 모니터링

다중 접속 기능

다중접속 기능은 전문가와 현장 담당자가 즉시 하나의 화면을 보며 협력하여, 출장 없이 신속하게 문제를 해결하는 글로벌 협업이 가능합니다.

여러 사용자가 한 장비에 동시 접속



듀얼 엔진 시스템

전 구간 암호화 통신

성능 모니터링

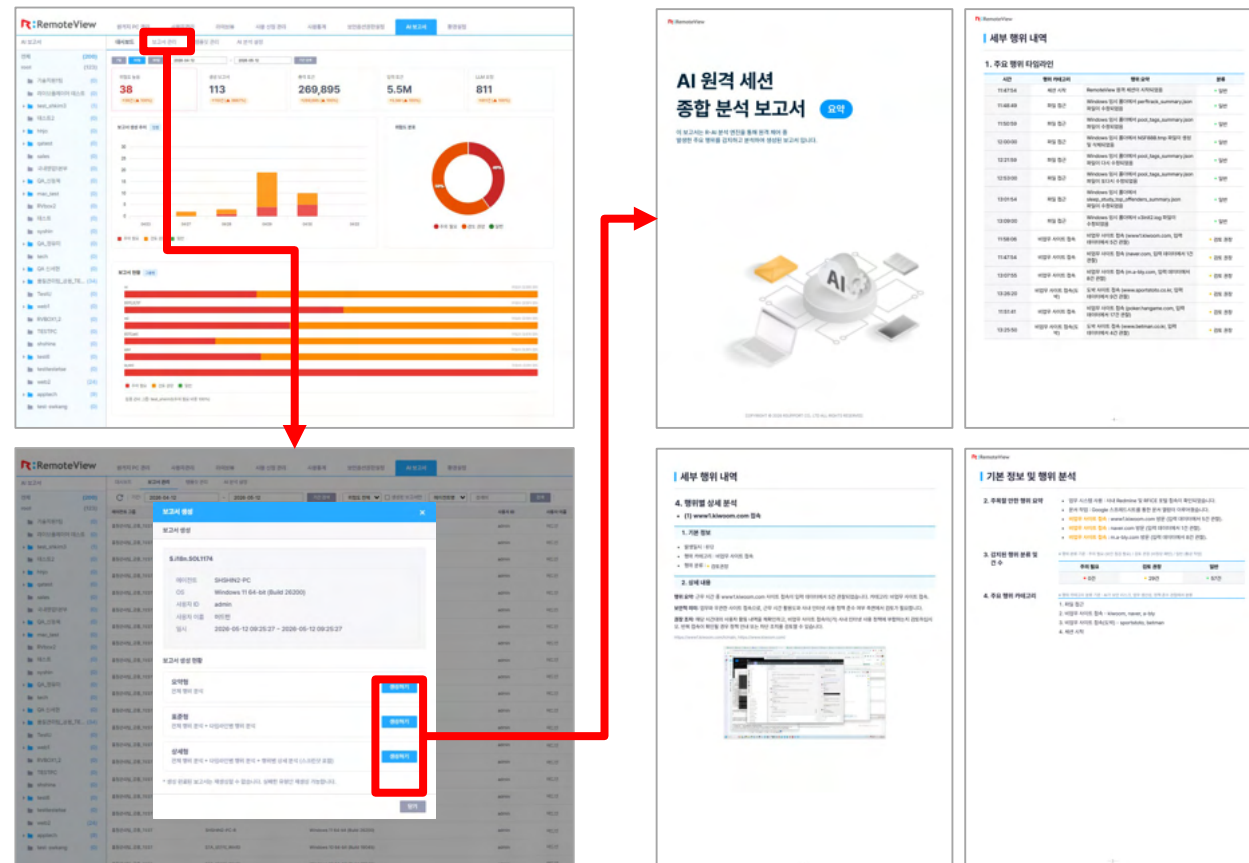
멀티 모니터 지원

다중 접속 기능

AI 보고서 및 모니터링

AI 보고서 및 모니터링

보안 정책에 의거하여, 사용자별 원격제어 녹화파일 분석을 하여, 위험도를 구분할 수 있으며, AI를 통해 원격 세션 종합 보고서로 생성할 수 있습니다.



2차 인증 로그인 및 접속 단말기 제한을 통한 보안 강화

OTP 인증을 통한 2차 인증 지원 및 IP/MAC 주소 원격제어 접속 제한을 통한 원격제어 보안이 가능합니다.

로그인 인증

The screenshot shows a login interface with a modal titled "2단계 인증" (2-step authentication). The modal contains the following text: "로그인을 완료하기 위해 2단계 인증이 필요합니다. Google OTP 앱을 실행하여 OTP 인증번호 6자리를 입력해 주세요." (To complete login, 2-step authentication is required. Please run the Google OTP app and enter the 6-digit OTP authentication number). Below the text is a text input field labeled "Google OTP 인증 번호 입력" (Enter Google OTP authentication number) and a blue "확인" (Confirm) button. At the bottom of the modal are two links: "2단계 인증이란?" (What is 2-step authentication?) and "메일로 인증키 수신" (Receive authentication key via email). A "닫기" (Close) button is located at the bottom center of the modal.

IP/MAC 주소를 통한 접속지역, 단말기 식별

The screenshot shows the "허용 IP, MAC 설정" (Allowed IP, MAC settings) page. It has two main sections: "허용 IP 설정" (Allowed IP settings) and "허용 MAC 설정" (Allowed MAC settings). Both sections have radio buttons for "전체사용" (All use), "사용자 설정" (User settings), and "사용안함" (Do not use). The "사용자 설정" option is selected in both. Below the "허용 MAC 설정" section, there is a link "엑셀파일로 일괄 업데이트" (Bulk update via Excel file) and a note: "등록할 사용자가 많은 경우 Excel 파일로 일괄 등록이 가능합니다." (In case of many users to be registered, bulk registration via Excel file is possible). There is also a section for "기본 MAC 주소" (Default MAC address) with "사용함" (Use) selected. Below this, there are two input fields for MAC addresses, each with a "삭제" (Delete) button. At the bottom, there is a "추가" (Add) button. The page also has a "보안 설정" (Security settings) section at the bottom with a radio button for "장기 미접속 에이전트 설정" (Long disconnection agent settings) set to "사용안함" (Do not use).

다양한 비밀번호 정책 설정 가능

보안 수준 별 비밀번호 정책 설정 및 비밀번호 사용기간을 설정할 수 있으며, 무차별 대입공격을 방어하기 위한 정책을 수립할 수 있습니다.

다양한 비밀번호 정책

비밀번호 보안 단계 설정	☒ 보안 수준 - 약 * 6~24자 이내 / 영문(대/소), 숫자, 특수문자 입력 가능 ☐ 보안 수준 - 중 * 8~24자 이내 / 영문(대/소), 숫자, 특수문자 입력 가능 * 연속적인 숫자 3자 이상 사용 불가 ☐ 보안 수준 - 강 (사용자 정의) * 8~24자 이내 / 영문(대/소), 숫자, 특수문자 입력 가능 * 연속적인 숫자 3자 이상 사용 불가 * 영문 대문자, 소문자, 숫자, 특수문자를 조합하여야 합니다.
비밀번호 사용 기간 설정	☐ 비밀번호 사용 기간 설정 5 일 (최소 1~90일로 설정)
비밀번호 입력 5회 실패 시 계정 잠금	☒ 전체사용 ☐ 사용안함 로그인 잠금 시간 설정 10 분 (0~99 사이의 숫자 입력) ☐ 관리자 계정 잠금 일 때만 메일 수신 비밀번호 입력 5회 실패 시 설정한 시간 동안 로그인을 제한하며, 관리자의 이메일로 알림 메일이 발송 설정된 시간 이후 다시 로그인을 시도할 수 있습니다. * 이메일이 등록되어 있지 않은 경우 알림 메일이 발송되지 않습니다.

1

비밀번호 보안 단계 설정

- 보안 수준 약/중/강을 통한 사용자 비밀번호 통제 및 관리

2

비밀번호 사용 기간 설정

- 1일~90일 비밀번호 사용기간 설정
* KISA 스마트공장 보안가이드 비밀번호 정책 충족

3

비밀번호 입력 실패 시 로그인 제한

- 무차별 비밀번호 대입 공격 예방 가능

원격제어 접속 외부 단말기 보안 상태를 체크하여 접근 통제

외부 단말기 원격제어 접속 시 필수 보안프로그램 설치유무, 화면보호기 설정 유무, OS 확인 및 업데이트 체크를 통한 외부 단말기의 보안 상태 점검 기능을 제공합니다.

외부 단말기 체크

알럿 창 팝업

전자금융감독규정 시행세칙 보안설정	
보안 프로그램 프로세스 검사	☐ 전제사용 ☒ 사용안함
원격 제어 가능 OS 설정	☐ 전제사용 ☒ 사용안함 사용자 측 PC에 OS(Windows, macOS) 버전이 낮으면 원격 연결이
OS 계정 비밀번호 설정 여부 검사	☒ 전제사용 ☐ 사용안함 사용자 측 PC에 OS(Windows, macOS) 계정 비밀번호가 설정되어 5
화면보호기 사용 설정 여부 검사	☒ 전제사용 ☐ 사용안함 사용자 측 PC에 화면보호기 사용 설정(Windows, macOS)이 되어 있 대기 시간 체크 설정 5 분(1-60 사이의 숫자 입력)
사용자 최초 로그인 시 비밀번호 변경	☒ 전제사용 ☐ 사용안함 관리자가 추가한 사용자가 최초 로그인 시, 비밀번호 재설정 후 서비스
SSL 인증서 체크 설정	☐ 전제사용 ☒ 사용안함 원격 연결 HTTPS 통신 시, SSL인증서를 체크하지 않도록 설정 할 수 있습니다. (완벽한 암호화 통신을 위해 '사용함' 상태 유지를 권장합니다.)
OS 최신 보안 패치 여부 검사	☒ 전제사용 ☐ 사용안함 사용자 측 PC OS(Windows)의 보안 패치 최신 여부를 검사합니다. (Windows 10 이상 지원 / Windows Server OS 미지원) 최신 보안 패치가 적용되지 않은 경우 원격 연결이 제한됩니다.
백신 설치 및 최신 업데이트 여부 검사	☒ 전제사용 ☐ 사용안함 사용자 측 PC(Windows)의 백신 설치 및 최신 업데이트 여부를 검사합니다. (Windows 10 이상 지원 / Windows Server OS 미지원) 백신 설치와 백신 최신 업데이트가 되지 않은 경우 원격 연결이 제한됩니다.
관리자 페이지 로그인 허용 IP 설정	☐ 전제사용 ☒ 사용안함

RemoteView

OS 계정 비밀번호 설정 확인

화면 보호기 사용 설정 확인

OS 최신 보안 패치 검사

백신 설치 및 최신 업데이트 여부 검사

새로고침

확인

OS 계정 비밀번호 설정 여부 확인

화면 보호기 설정 여부 확인

사용자 최초 로그인 시 비밀번호 변경

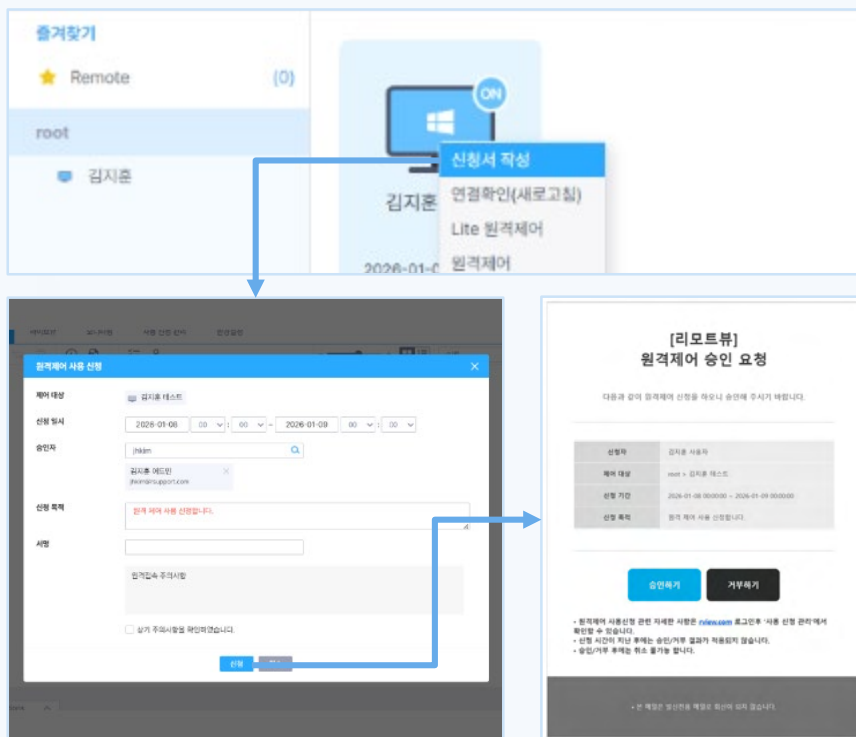
OS 최신 보안 패치 여부 검사

백신 설치 여부 및 실시간 업데이트 확인

원격제어 신청(보안서약서)

원격제어 사용 신청 기능을 통해 원격제어 시 보안서약서 징구하고, 허가 받지 않은 사용자들의 접속을 통제합니다.
사용 요청은 관리자 메일주소 및 관리자페이지 에서 승인 및 거부 할 수 있습니다.

원격제어 신청 프로세스



원격제어 신청 승인 및 관리

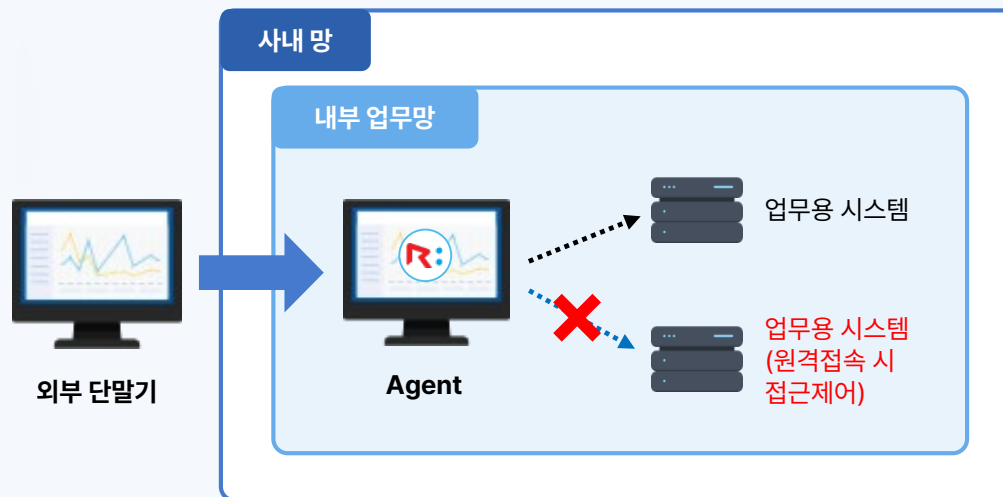
승인자	승인 일시	신청 목적	사용 승인	사용 확인
김지훈 어드민	-	원격 제어 사용 신청합니다.	승인 거부	
승인자	승인 일시	신청 목적	사용 승인	사용 확인
김지훈 어드민	-	원격 제어 사용 신청합니다.	대기	-
어드민	-	원격접속	대기	-
어드민	2025-12-04 09:47:56	사유를 명확하고 구체적으로 기입하여 주시기 바랍니다. (부적절하게 기입할 경우 감사 대상이 될 수 있습니다.)	승인 완료	확인
어드민	2025-12-04 09:42:20	사유를 명확하고 구체적으로 기입하여 주시기 바랍니다. (부적절하게 기입할 경우 감사 대상이 될 수 있습니다.)	승인 완료	확인
어드민	2025-12-03 16:20:13	사유를 명확하고 구체적으로 기입하여 주시기 바랍니다. (부적절하게 기입할 경우 감사 대상이 될 수 있습니다.)	승인 완료	확인
어드민	2025-12-03 16:18:52	사유를 명확하고 구체적으로 기입하여 주시기 바랍니다. (부적절하게 기입할 경우 감사 대상이 될 수 있습니다.)	승인 완료	확인 완료
어드민	2025-12-03 16:12:28	사유를 명확하고 구체적으로 기입하여 주시기 바랍니다. (부적절하게 기입할 경우 감사 대상이 될 수 있습니다.)	승인 완료	미사용
어드민	2025-12-03 15:56:14	사유를 명확하고 구체적으로 기입하여 주시기 바랍니다. (부적절하게 기입할 경우 감사 대상이 될 수 있습니다.)	승인 완료	확인
어드민	2025-12-03 15:14:50	사유를 명확하고 구체적으로 기입하여 주시기 바랍니다. (부적절하게 기입할 경우 감사 대상이 될 수 있습니다.)	승인 완료	확인

외부 원격 접속 시 특정 프로그램 및 시스템 접근제어

접근 제어가 필요한 시스템 또는 URL을 통제함으로써 보안유출 리스크를 감소할 수 있습니다.

내부 접근 통제

- 원격제어 시 내부 중요 시스템에 대한 접근 통제 기능 제공
- 프로세스, 서비스 제어를 통한 접근 통제
- URL 주소 제어를 통한 접근 통제



원격지 PC 실행 제한 설정

원격지 PC 프로세스 중지 설정

☒ 전체사용 ☐ 사용안함

원격제어 시, 사용자가 등록한 프로세스를 실시간으로 모니터링하여 중지시킵니다.

- 원격제어 시, 원격지PC에서 중지하고자 하는 프로세스명을 정확히 입력해주세요.
- 운영체제(OS) 관련, Remote View 관련 프로세스 등록 불가
- 파일명을 .exe 형태로 입력해 주세요.
- Windows PC만 지원합니다.

원격지 PC 서비스 중지/재실행 설정

☐ 전체사용 ☒ 사용안함

원격지 PC 웹 URL 차단 설정

☐ 전체사용 ☒ 사용안함

파일 보내기 / 받기 기능을 통한 자료유출 차단

원격제어 시 파일로 인한 악성코드 감염을 예방할 수 있으며 자료유출을 방지할 수 있습니다.

파일 보내기 / 받기 기능

파일 전송 설정  

제어 중 파일 전송 설정

☒ 파일 송수신 (보내기, 가져오기)
☐ 파일 송신 (보내기)
☐ 파일 수신 (가져오기)
☐ 사용안함

원격제어 시 단말기 간에 파일송수신(보내기, 가져오기) 여부를 설정합니다.

파일 전송 용량 설정

☒ 무제한 ☐ 직접입력

원격탐색기 사용

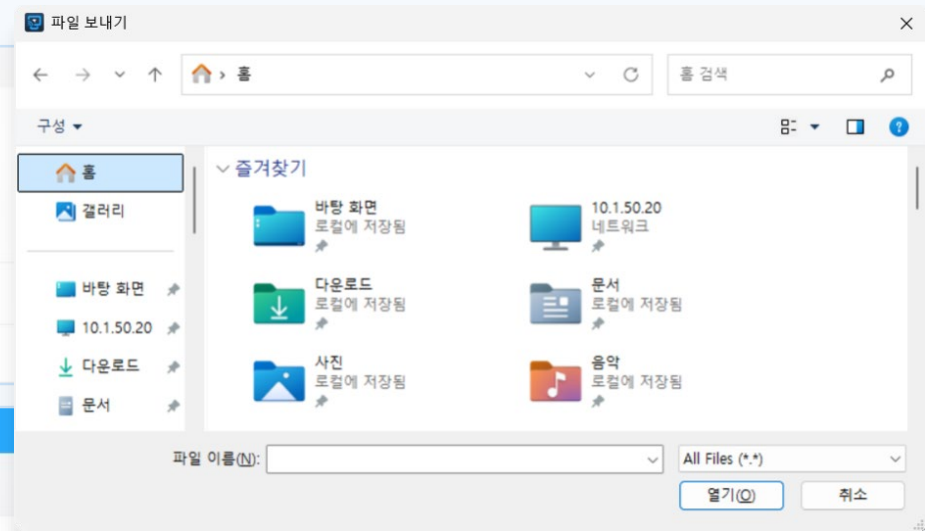
☐ 전체사용 ☒ 사용안함

사용자 권한 설정

그룹 선택을 하시면 에이전트 선택이 활성화 됩니다.
에이전트선택에서 "선택하지 않음"은 해당 그룹에 권한 할당 시 사용됩니다.

그룹 선택*

이름	☒ 원격탐색기	☒ 원격제어	☒ 다중접속 사용	☒ 원격화면캡처	☒ 프린트	☒ 녹화	☒ 파일 송수신	☒ 클립보드
 jhkim	☒ 허용	☒ 허용	☒ 허용	☒ 원격화면캡처	☒ 프린트	☒ 녹화	☒ 파일 송수신	☒ 클립보드



파일전송 이력 확인 기능을 통하여 파일 전송시작 / 종료 시간, 파일명, 크기, 성공여부를 확인합니다.

- 전송시작 시간
- 전송종료 시간
- 송수신 종류
- 파일명, 파일크기
- 성공여부

리

라이브뷰

모니터링

사용 통계

보안음성권한설정

환경설정

전송

노출 항목 설정

최근 제어 날짜

2025-12-08

~

2026-01-0

Command	ClientAccessPrivatop	ClientAccessPublicip	AgentGroupName	AgentName	AgentOsName	AgentPrivateIp	AgentPublicip	StartDate
REMOTECONTROL	10.2.3.29	220.85.141.73	root	EHSONG-PC2	Windows 10 64-bit	172.19.161	10.1.73.25	2025-12-18 11:02
AGENTUNINSTALL		10.1.71.75	test1	JSSHIN-PC	Windows 11 64-bit	169.254.202.56	220.85.141.71	2025-12-18 09:09
AGENTUNINSTALL		10.1.71.75	test1	JSSHIN-PC	Windows 11 64-bit	169.254.202.56	220.85.141.71	2025-12-18 09:09
AGENTUNINSTALL		10.1.73.25	root	EHSONG-PC2	Windows 10 64-bit	172.19.161	220.85.141.73	2025-12-18 09:09
REMOTECONTROL	10.1.71.75	220.85.141.71	TQC	JSSHIN-PC	Windows 11 64-bit	192.168.0.175	220.85.141.71	2025-12-17 23:14
AGENTUNINSTALL								2025-12-17 23:14
REMOTECONTROL								2025-12-17 18:02
REMOTECONTROL								2025-12-17 15:44
INVITESUCCESS								2025-12-17 15:44
REMOTECONTROL								2025-12-17 15:44
REMOTECONTROL								2025-12-17 15:02
REMOTECONTROL								2025-12-17 14:56
REMOTECONTROL	10.1.71.75	220.85.141.71	TQC	VPRO-40EJSQU	Windows 10 64-bit	10.180.39	220.85.141.80	2025-12-17 14:56
REMOTECONTROL	10.1.71.75	220.85.141.71	TQC	VPRO-40EJSQU	Windows 10 64-bit	10.180.39	220.85.141.80	2025-12-17 14:56
REMOTECONTROL	10.1.71.75	220.85.141.71	TQC	VPRO-40EJSQU	Windows 10 64-bit	10.180.39	220.85.141.80	2025-12-17 14:56
REMOTECONTROL	10.2.3.29	220.85.141.73	root	EHSONG-PC2	Windows 10 64-bit	172.19.161	10.1.73.25	2025-12-18 10:21
AGENTUNINSTALL		10.1.71.75	test1	JSSHIN-PC	Windows 11 64-bit	169.254.202.56	220.85.141.71	2025-12-18 09:09
AGENTUNINSTALL		10.1.71.75	test1	JSSHIN-PC	Windows 11 64-bit	169.254.202.56	220.85.141.71	2025-12-18 09:09
AGENTUNINSTALL		10.1.73.25	root	EHSONG-PC2	Windows 10 64-bit	172.19.161	220.85.141.73	2025-12-18 09:09
AGENTUNINSTALL		10.1.71.75	TQC	JSSHIN-PC	Windows 11 64-bit	192.168.0.175	220.85.141.71	2025-12-17 23:14

파일전송 이력

파일전송 이력

전송 시작시간

전송 종료시간

송수신

파일명

파일 크기

성공 여부

2025-12-17 15:04:03

2025-12-17 15:04:03

파일 수신 (가져오기)

test - 복사본.txt

4

true

2025-12-17 15:04:03

2025-12-17 15:04:03

파일 송신 (보내기)

test - 복사본.txt

4

true

닫기

원격 탐색기 기능을 통한 파일관리

원격제어를 하지 않고, 원격지 PC의 파일 송수신이 가능합니다.

원격 탐색기 기능

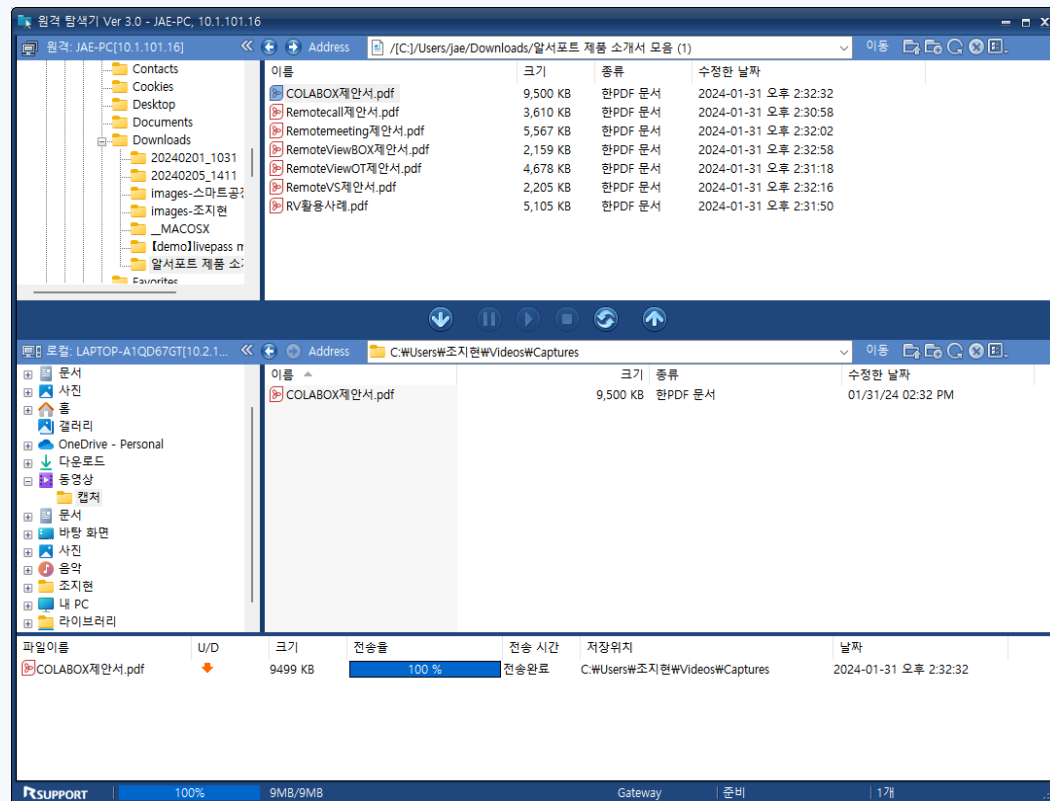
최고 사양의 FTP 성능 개선

서버 파일 관리 및 파일 전송

멀티 파일 전송 - 다중 파일 전송

파일 Search 기능

Drag and Drop, Ctrl+C/V 기능 지원



자료유출 보안용 워터마크 기술 제공

외부 단말기에서 원격제어 시 사진 촬영, 캡처를 이용한 자료유출을 방지하기 위해 워터마크 기능을 제공합니다.

원격제어 화면 유출방지

캡처방지를 통한 불법유출 차단

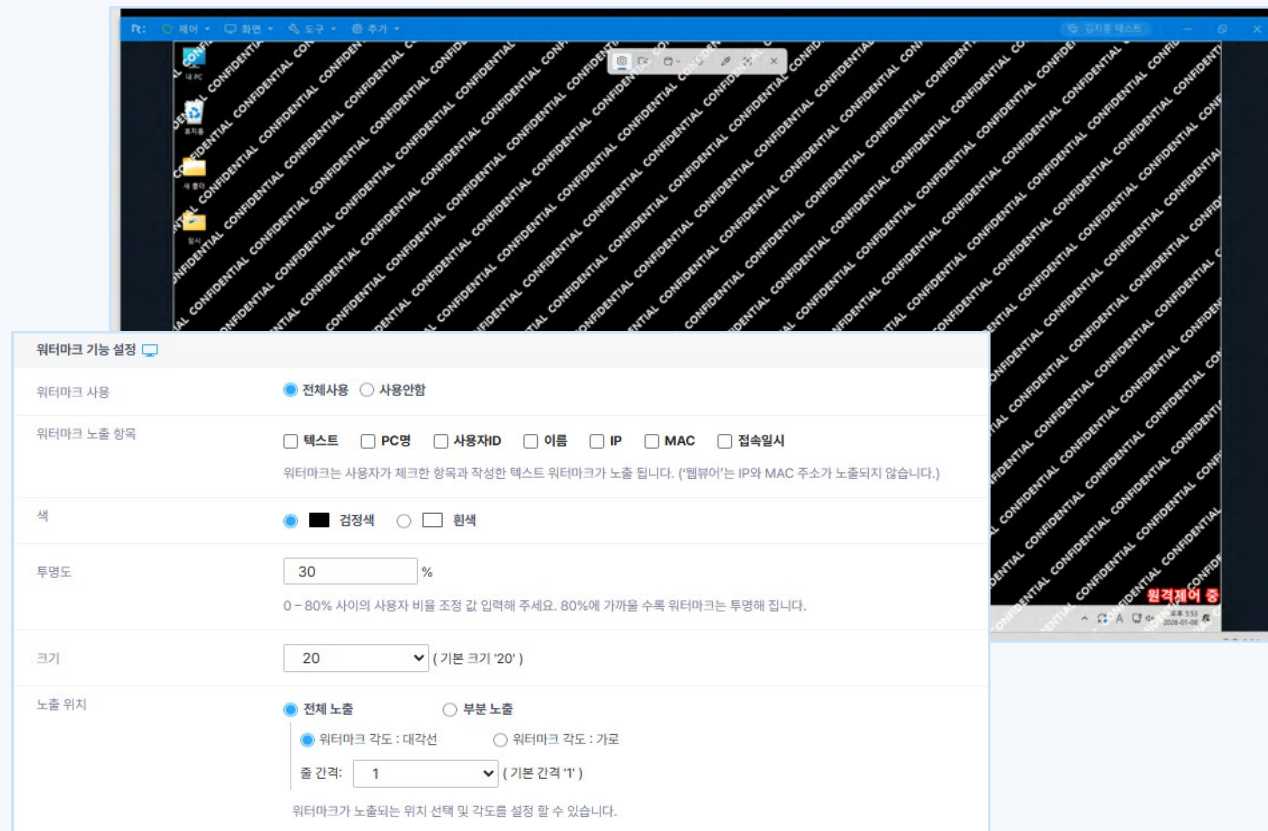
- 원격접속 사용자 정보(ID, IP, 접속일시, MAC주소)를 통한 사용자 식별
- 전화번호, 부서명, 이름 등 접속자 정보

키보드 잠금을 통한 캡처 통제

- 비활성화를 통한 캡처 방지

다양한 워터마크 옵션 설정

- 글씨 색상, 투명도, 크기, 노출 위치 등



원격지 모니터 잠금 기능으로 나의 업무 프라이버시 보호

원격 PC의 모니터 화면 잠금 기능을 사용하여 제어중인 원격 PC의 화면을 가려 다른 사용자에게 중요한 정보가 노출되는 것을 방지할 수 있습니다.

원격지 PC의 모니터 / 키보드 / 마우스 잠금



원격지 PC

원격 화면 잠금

- PC의 화면을 잠금 설정하여 타인이 원격제어 중인 화면을 볼 수 없음
- 다양한 화면 잠금방식 제공
(모니터 OFF, 모니터 드라이버 OFF, Black Layer 방식)

원격 키보드 / 마우스 잠금

- PC의 키보드와 마우스를 잠금 설정하여 타인의 임의 조작 방지

원격제어내역 녹화 및 로그 보관을 통한 보안관리

원격제어 이후 전수 녹화파일을 서버에 저장하며 유출되더라도 외부에서 재생이 불가능합니다.

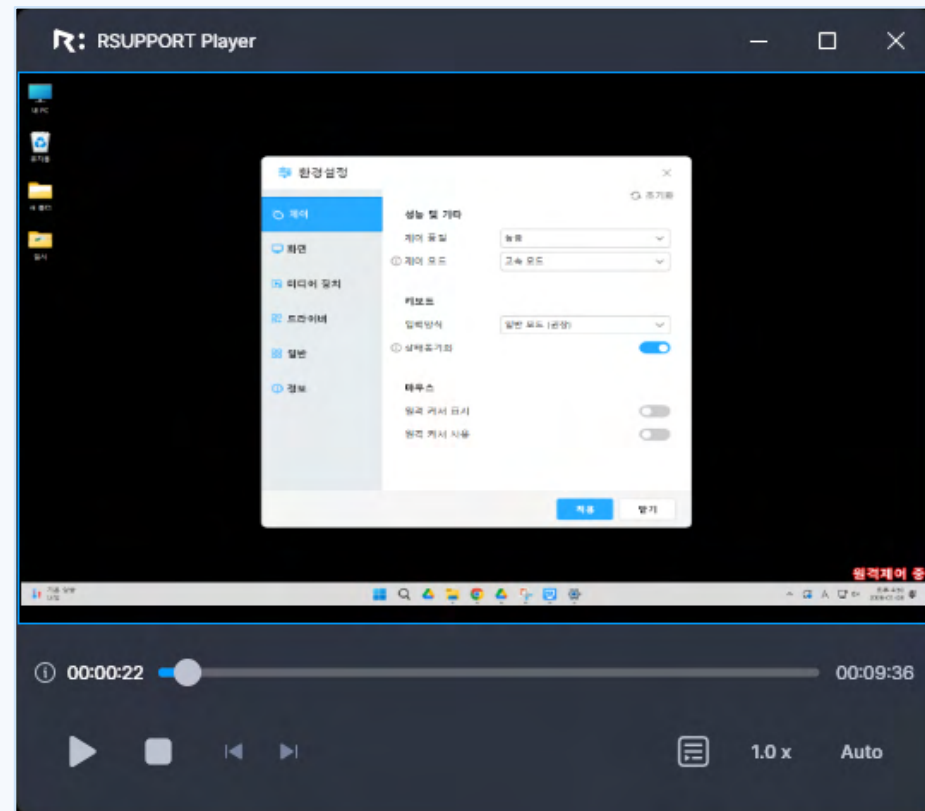
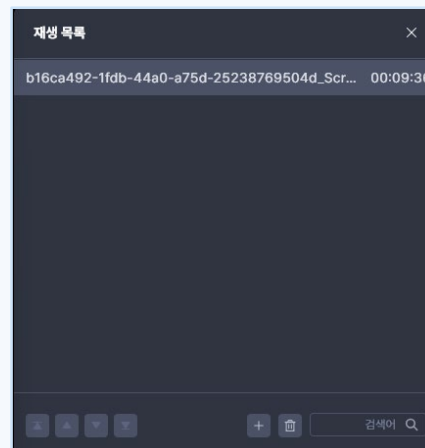
녹화파일 용량

기계 1Unit 기준

- 1분 : 1MB ~ 5MB
- 1일(9시간) : 0.5GB ~ 2.6GB
- 1달(20일) : 10.5GB ~ 52.7GB

기계 100Unit 기준

- 1분 : 100MB ~ 500MB
- 1일(9시간) : 53GB ~ 263GB
- 1달(20일) : 1TB ~ 5TB



원격제어 이력과 실시간 차트를 통한 시각화

시각화된 통계 차트와 상세 원격제어 이력을 통해 원격 접속을 투명하게 모니터링합니다.

접속로그 보관 가이드라인

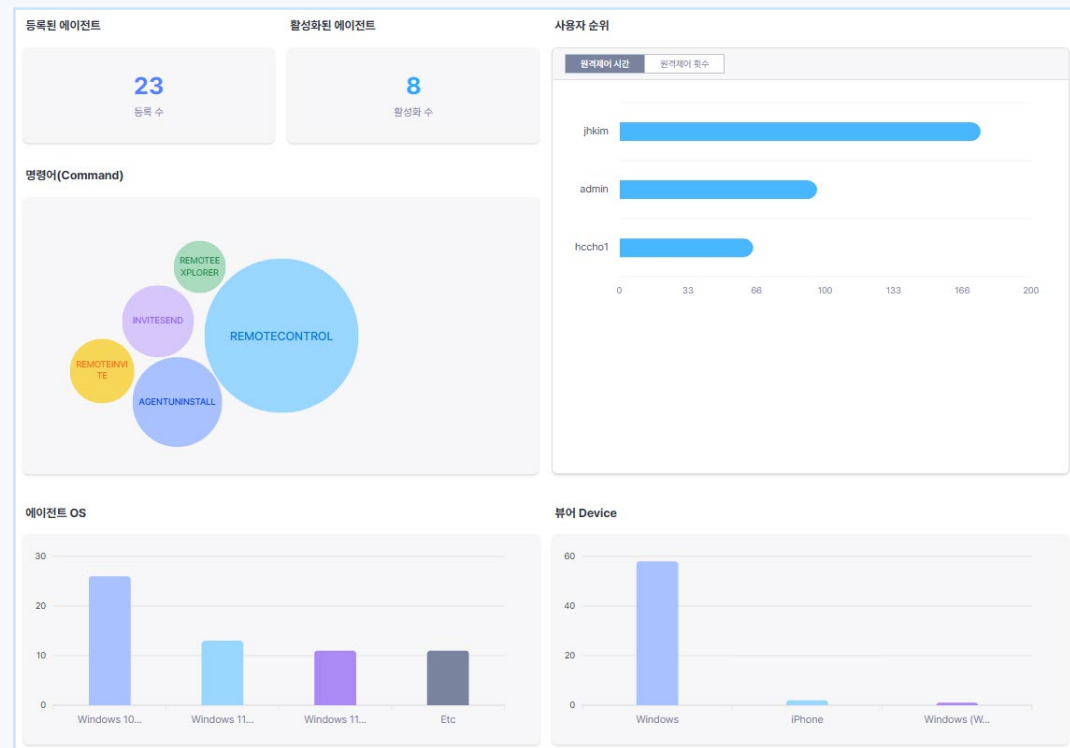
원격제어 기록

- 원격제어 사용자의 정보
- 접속 일시
- 접속한 내부 시스템
- 내역은 일정기간 보관

원격제어 이력

CreateDate	UserId	Name	RequestDevice	Command	ClientAccessPrivateIp	ClientAccessPublicIp	AgentGroupName
2026-01-08 17:36:23	jhkim	김지훈 사용자	Windows	REMOTECONTROL	10.2.52.25	220.85.141.52	root
2026-01-08 16:39:01	jhkim	김지훈 사용자	Windows	INVITESEND	10.2.52.25	220.85.141.52	root
2026-01-08 16:26:56	jhkim	김지훈 사용자	Windows	REMOTECONTROL	10.2.52.25	220.85.141.52	root
2026-01-08 16:15:54	jhkim	김지훈 사용자	Windows	REMOTECONTROL	10.2.52.25	220.85.141.52	root
2026-01-08 15:28:40	jhkim	김지훈 사용자	Windows	REMOTECONTROL	10.2.52.25	220.85.141.52	root
2026-01-08 15:26:41	jhkim	김지훈 사용자	Windows	REMOTECONTROL	10.2.52.25	220.85.141.52	root
2026-01-08 15:25:30	jhkim	김지훈 사용자	Windows	REMOTECONTROL	10.2.52.25	220.85.141.52	root
2026-01-08 15:24:41	jhkim	김지훈 사용자	Windows	REMOTECONTROL	10.2.52.25	220.85.141.52	root
2026-01-08 15:24:40	hccho1	조한철	Windows	INVITESEND	10.2.52.25	220.85.141.52	root
2026-01-08 15:24:00	jhkim	김지훈 사용자	Windows	REMOTECONTROL	10.2.52.25	220.85.141.52	root

차트



원격제어 현황을 한눈에 관리할 수 있는 라이브뷰

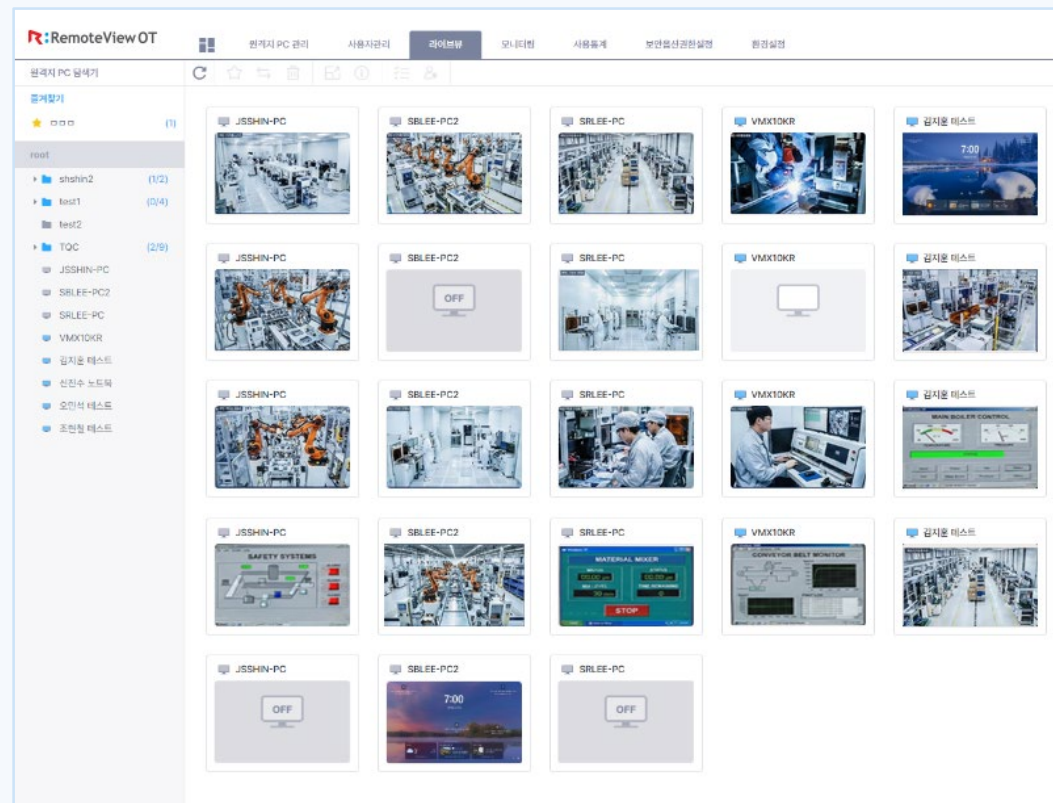
다수의 PC를 한눈에 관리할 수 있으며 장비의 문제 발생 시 바로 확인 및 해결 가능합니다.

자동화 설비 기기에 대한 모니터링

원격 모니터링 중 이상 화면 발생 시
즉시 인지 및 대처 가능

5초 단위 화면 갱신으로 화면 표출

시스템 장애 발생시 바로 원격으로
작업하여 장애 시간 최소화



라이브뷰 전용 대시보드(옵션)

라이브뷰 전용 대시보드를 통해 사용자의 모니터링 환경에 맞춰 유연하게 대응 가능합니다.

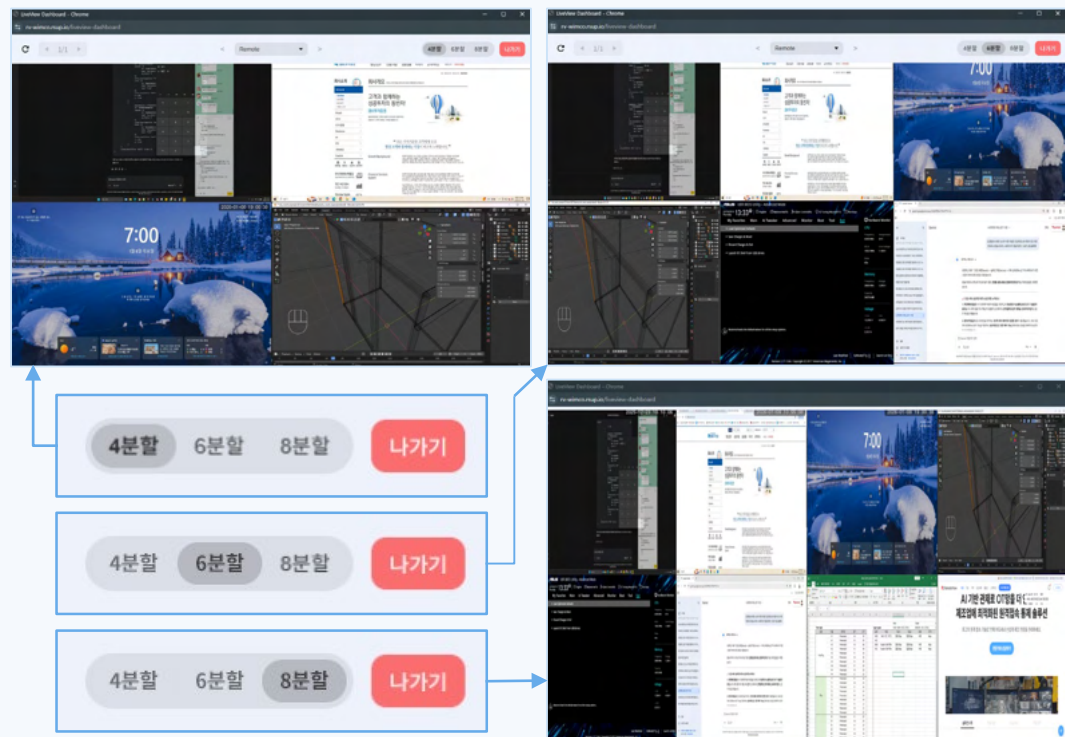
에이전트 그룹별 · 분할 화면별 라이브뷰 모니터링



존 라이브뷰 인터페이스를 고도화하여, 다분할 레이아웃으로 실시간 고밀도 통합 관제 환경이 가능합니다.

즐거찾기를 통해 맞춤형 집중 관리가 가능합니다.

시스템 연동을 통한 즉각적인 통합 관제가 가능합니다.



사용자 계정 권한 관리를 통한 편의성 제공

관리자를 통한 매니저 또는 사용자를 추가하여 인가된 사용자만 안전한 원격제어를 할 수 있으며, 부서별 / 업무별 / 기기별 그룹화를 통하여 사용자의 편의성을 제공합니다.

권한에 따른 사용자 분리 (사용자 - 관리자)

사용자 권한 설정

그룹 선택을 하시면 에이전트 선택이 활성화 됩니다.
에이전트 선택에서 "선택하지 않음"은 해당 그룹에 권한 할당 시 사용됩니다.

그룹 선택*
root

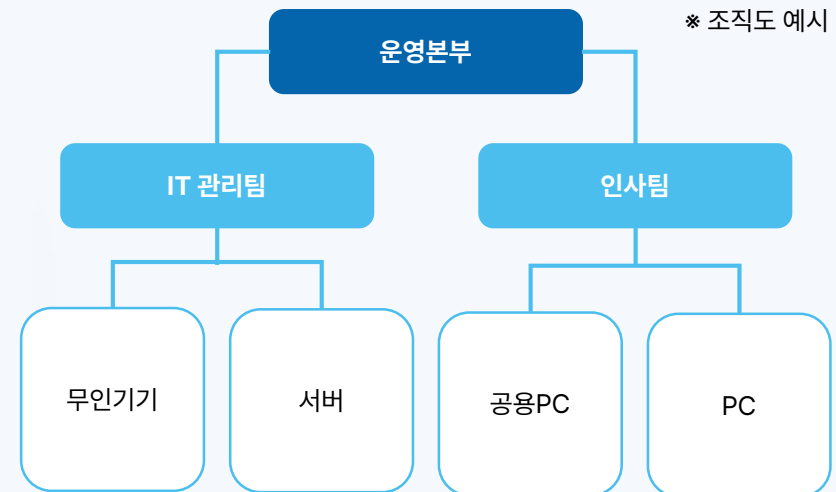
입력 또는 선택하세요.

에이전트 선택
입력 또는 선택하세요.

이름	그룹	원격화면캡처	프린트	녹화	파일 송수신
JSSHIN-PC					
SBLEE-PC2					
SRLEE-PC					
VMX10KR					
김지은 테스트					
신진수 노트북					
오민석 테스트					
조현철 테스트					
jnkim	허용	허용	허용	허용	허용
jnkima	허용	허용	허용	허용	허용
mssunga	허용	허용	허용	허용	허용
mssungd	허용	허용	허용	허용	허용

적용 취소

조직별 / 업무별 / 기기별 그룹화 관리

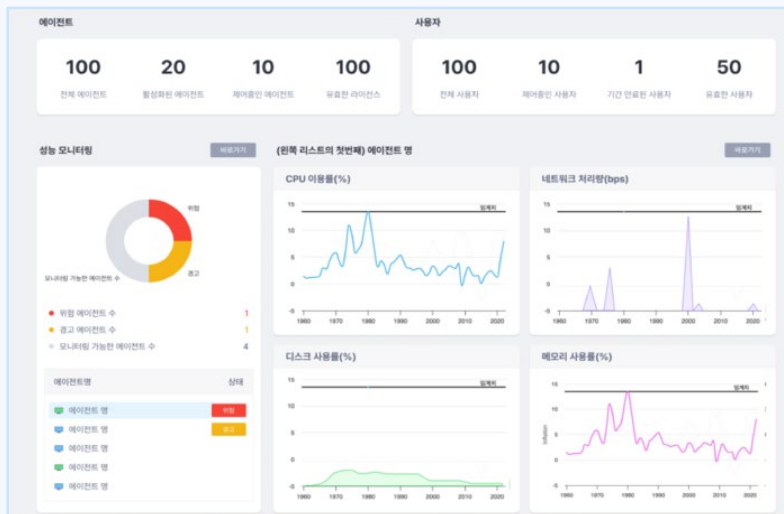


- **관리 포인트 관리** : 본사, 지사 등 거점 별 관리
- **업무 및 종류 관리** : 기업의 조직도와 동일한 사용자 그룹 구성
- **사용 기기 관리** : 기기의 장소, 종류(PC, Kiosk, 태블릿 등) 관리

대시보드 및 모니터링 (통합)

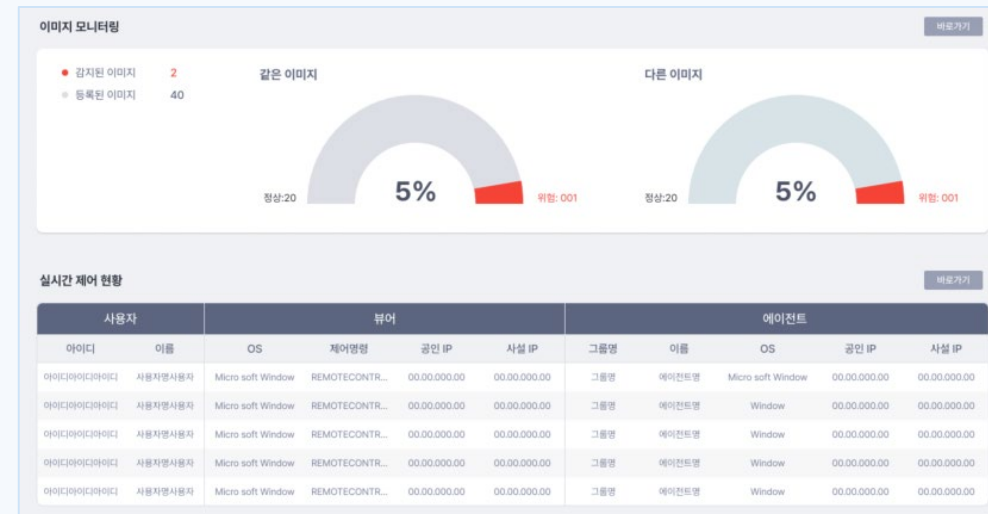
관리자는 사용자수, 등록된 에이전트수, 유효한 라이선스 수 등 한 눈에 확인이 가능합니다.

대시보드



- 에이전트 배포 현황을 직관적으로 확인
- 원격 접속자 및 로그인 사용자 현황을 실시간으로 모니터링
- 최근 사용 패턴을 분석하여, 어느 부서/사용자가 원격 접속을 많이 활용하는지 파악

이미지 모니터링

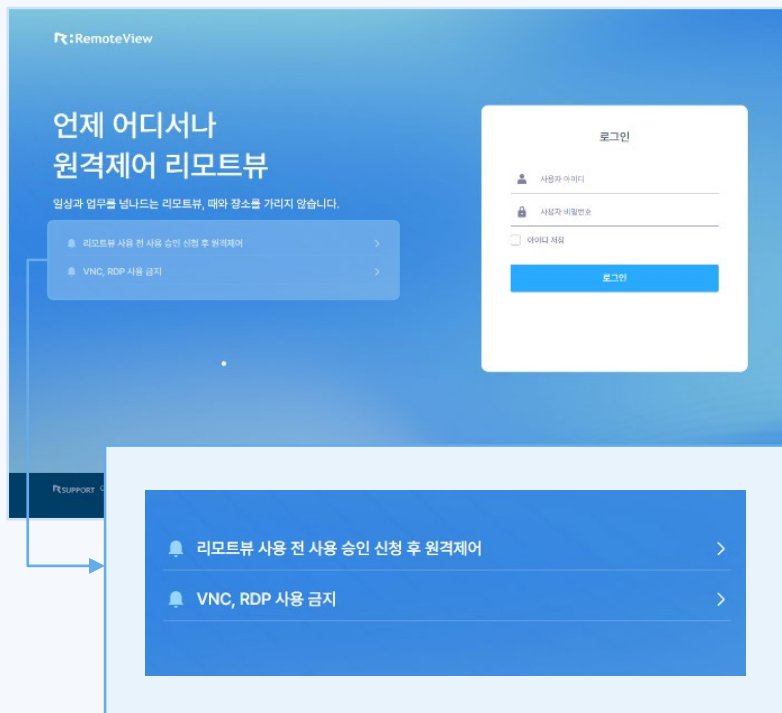


- 원격 접속 빈도 및 이용량을 수치화 관리
- 서버의 운영 상태를 대시보드 형태로 한눈에 확인
- 원격지 PC 화면을 등록한 이미지와 자동 비교하여 이상 여부를 감지하는 이미지 모니터링 기능을 제공

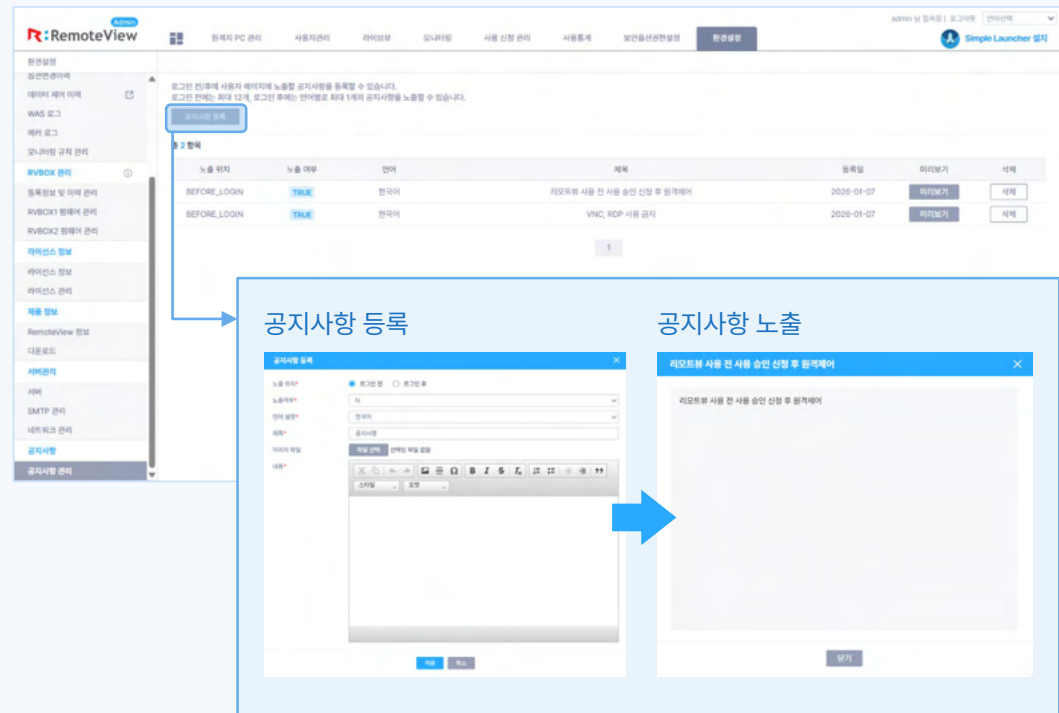
공지사항 기능

관리자는 사용자 로그인 전, 후에 원하는 내용으로 팝업 공지를 노출할 수 있습니다.

로그인 페이지 공지



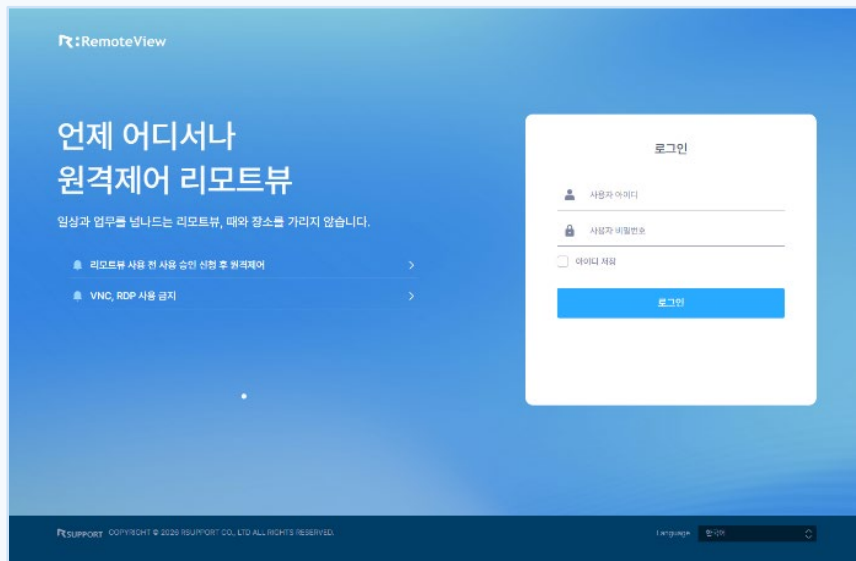
공지사항 이력관리



관리자 페이지 제공

관리자 전용 UI 및 접근 제어로 비인가 접근을 차단하여 운영 관리 및 보안성을 강화합니다.

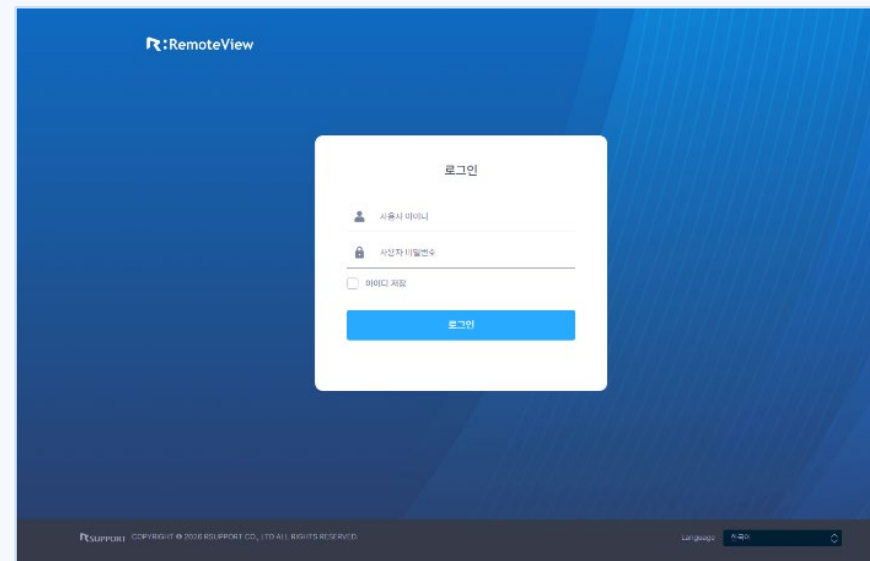
사용자 페이지



외부망에서도 접근 가능

- 원격제어 실행
- 원격제어 사용 신청/승인
- 원격제어 방식 설정

관리자 페이지



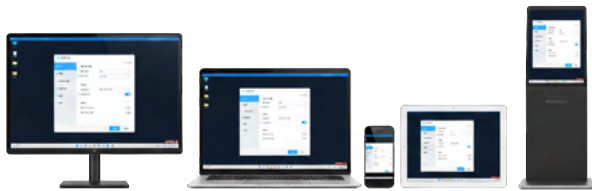
내부망에서만 접근 가능

- 원격제어 정책 설정
- 제어 이력 확인
- 사용자 계정 관리
- 특정 IP만 접근 가능

다양한 OS 및 기기 지원

RemoteView OT는 기기나 OS를 가리지 않으며 어떠한 환경에서도 강력한 원격제어가 가능합니다.

다양한 기기



다양한 OS



Windows



Mac



Android

iOS

iOS

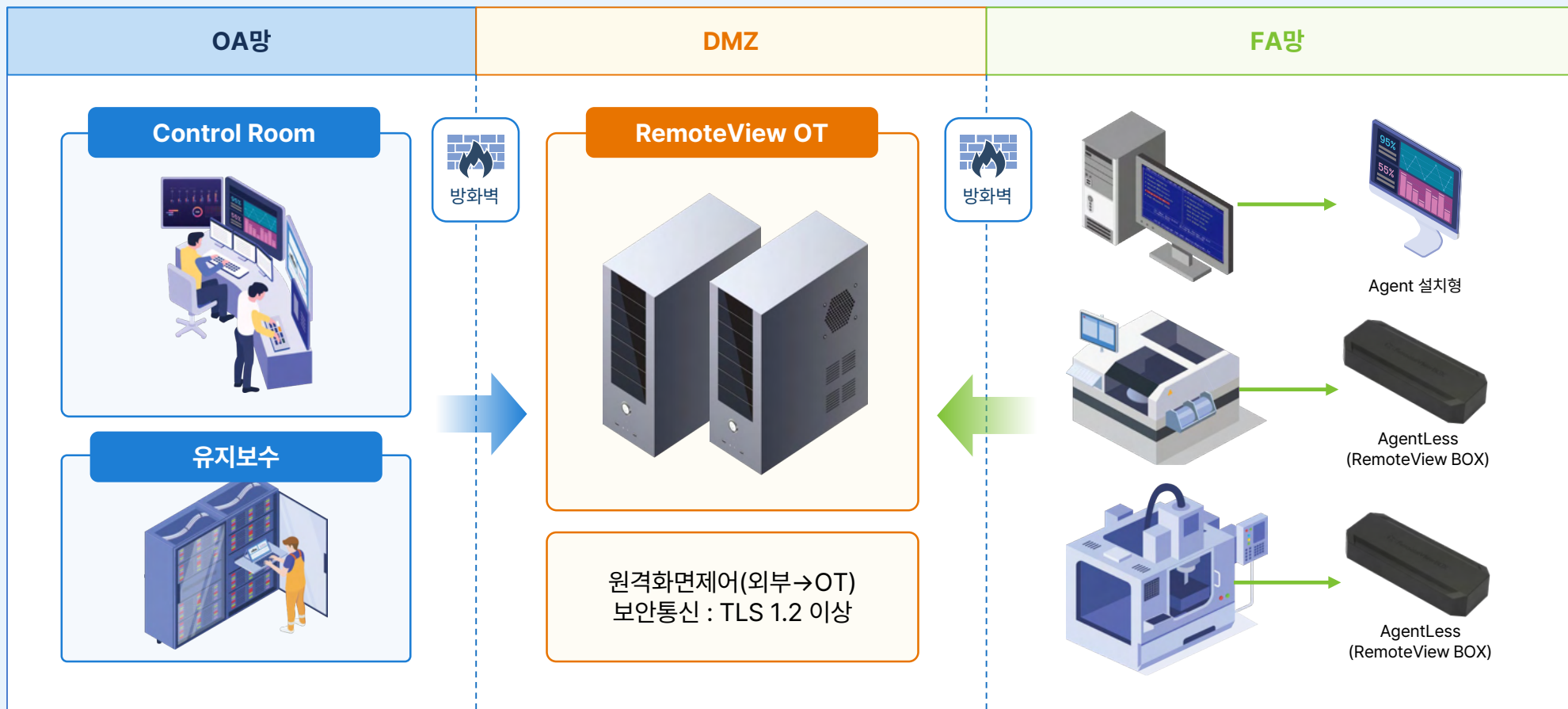
다양한 브라우저



운영체제	Window OS	Mac OS	Linux	Google Android	iOS
PC	Windows Server 2012 이상 Window 10 이상 (32bit, 64bit 지원)	Mac OS X 12이상	Cent OS 7.0~7.7(64 bit), Redhat OS 7.0~7.7(64bit) Ubuntu 14.4~18.4(64bit) 한컴OS Gooroom 2.2, TMax OS 21(에이전트 한함)	Android 8 이상	iOS 15 이상(뷰어)
Mobile	Android 8 이상	iOS 15 이상(뷰어)	-	Android 8 이상	N/A
고객 웹 브라우저	Microsoft Edge 90 이상 Mozilla Firefox 70 이상 Google Chrome 80 이상	Apple Safari 11 이상 Google Chrome 42 이상 Mozilla Firefox 38 이상	-	-	-

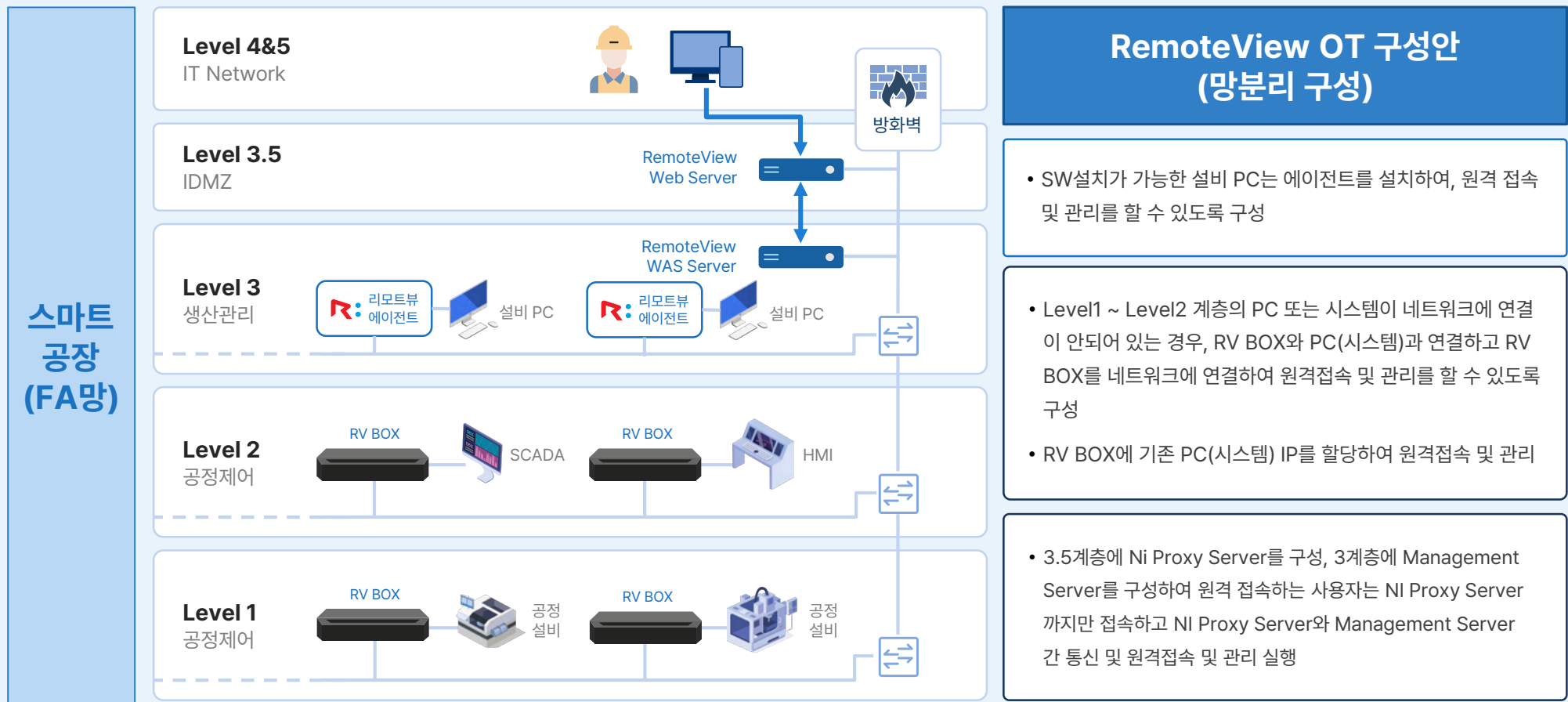
어떠한 네트워크 환경에서도 안전한 원격제어가 가능

OT망과 OA망 간 통신을 통해 PC를 안전하게 원격제어가 가능합니다.



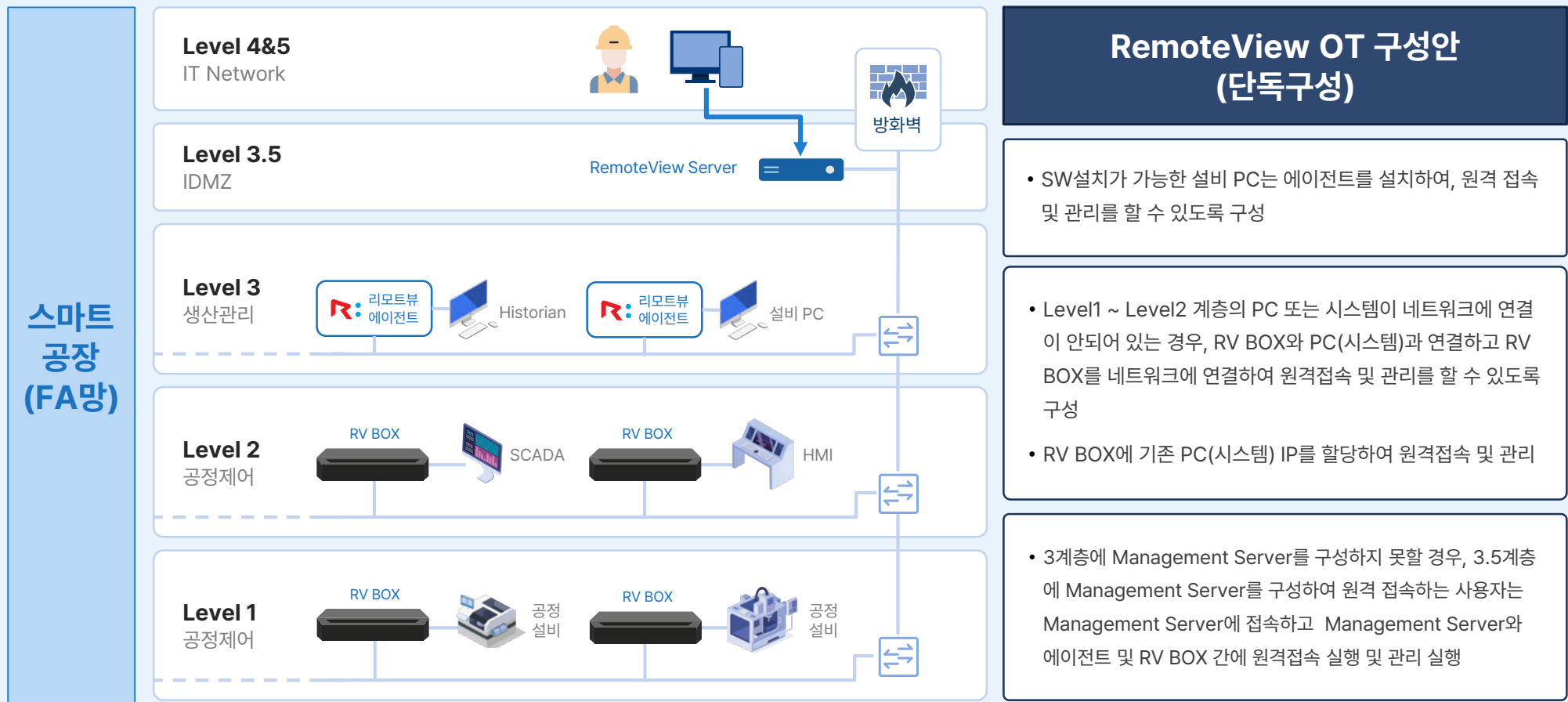
어떠한 네트워크 환경에서도 안전한 원격제어가 가능

OT망과 OA망 간 통신을 통해 PC를 안전하게 원격제어가 가능합니다.



어떠한 네트워크 환경에서도 안전한 원격제어가 가능

OT망과 OA망 간 통신을 통해 PC를 안전하게 원격제어가 가능합니다.



무결성 체크를 통한 안전한 파일 전송

제어대상 PC와 외부 업무 PC 간 파일 송수신 시, 백신 바이러스 체크를 통해 파일의 무결성 검사를 하여 안전한 파일전송 환경을 조성합니다.

파일 무결성 체크 효과

악성코드 피해 및 사이버 리스크 경감

보안사고 예방 및 데이터 자산 보호

안정적인 공장 IT System 운영가능

파일 무결성 체크 프로세스



RemoteView OT 전용 H/W

DMZ/외부망에 분리 구성, 2대의 H/W 간 통신을 통해 PC를 안전하게 원격제어가 가능합니다.

Rsupport H/W Pack

R:RemoteView OT

Rsupport HW Pack

*동시접속 사용자 200명 지원



구분	RemoteView Server
Chassis	3.5인치 새시 최대 4 핫 플러그 하드 드라이브, 어댑터 PERC 11
CPU	인텔® 제온® 6 성능 6333P 3.1G, 6C/12T, 18M 캐시, 터보, (65W)DDR5-4800
Memory	1×16GB UDIMM, 5600MT/s ECC
HDD	2×2TB 하드 드라이브 SATA 6Gbps 7.2K 512n 3.5인치 핫플러그
Power	듀얼, 핫 플러그 전원 공급 장치, 600W
WAS	Tomcat 9
DBMS	MariaDB 10
O/S	Rocky Linux 9
Size	1U, W482×D585.3(베젤 제외)~598.9(베젤 포함)×H42.8mm

On-Cloud 구축

사내 서버 구축이나 장비 구매 대신 클라우드 리소스를 빌려 사용하여 비용이 절감되고 유지보수가 간편합니다.

서버 운영 및 관리에 대한 부담을 줄여주는 구축형 클라우드 원격제어

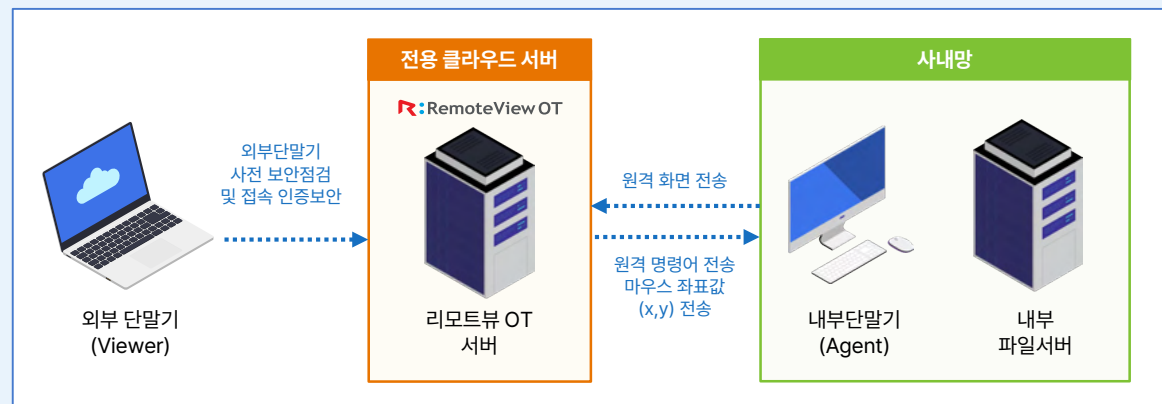
R:RemoteView OT

ON-Cloud

클라우드 구축형 솔루션



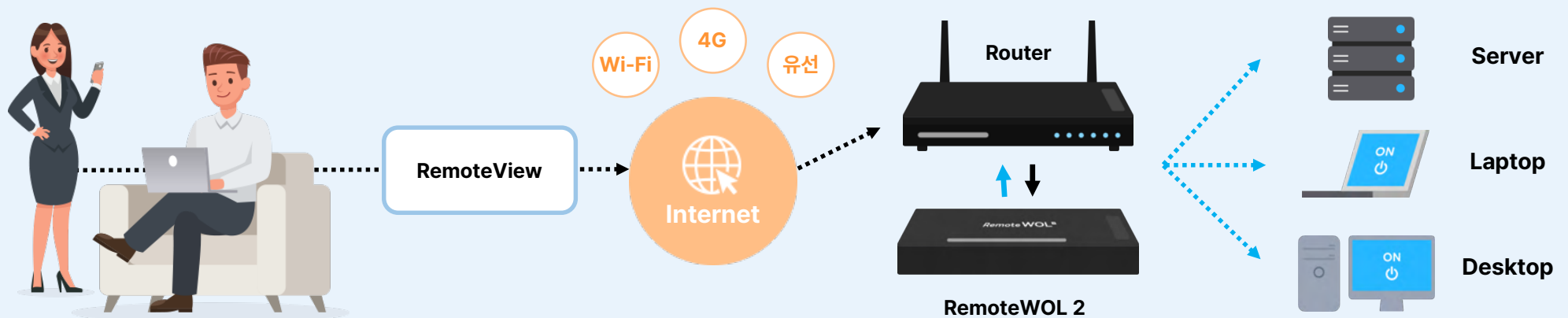
- 리모트뷰 OT 라이선스 모든 기능 지원
- 부담없는 초기 구축 비용
- 알서포트에서 고객사 전용 서버 및 유지보수 올인원 관리
- 대규모 보안 전문가 보유한 클라우드 서비스 이용으로 높은 보안성
- 전자금융감독규정 시행세칙 준수한 원격제어 구축
- 커스터마이징 유연성 용이



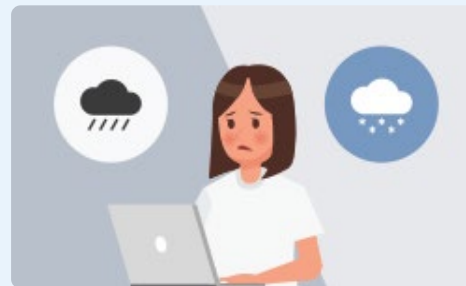
RemoteWOL을 이용하여 원격지 PC 전원 관리

RemoteWOL 제품으로 전원이 꺼져 있는 컴퓨터나 서버의 전원을 켜야 할 때 전원 제어를 할 수 있습니다.

꺼져있는 PC를 한번에 ON 시켜주는 RemoteWOL



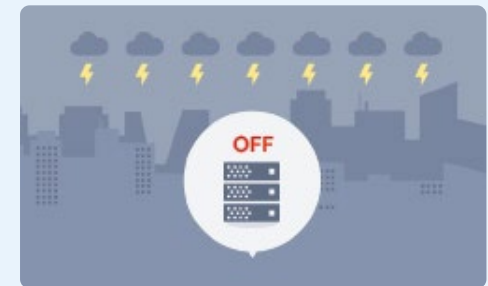
외근 / 출장 중 회사의
PC를 원격제어 해야할 때



폭설 / 장마 등 자연재해로
출근을 할 수 없을 때



다수의 PC를 켜야할 때



낙뢰로 서버의 전원이 꺼졌을 때

RemoteView BOX

저사양 PC 및 노후화된 OS기기까지도 RemoteViewBOX만 연결하면 프로그램 설치 필요 없이 사용할 수 있습니다.

RemoteView BOX란?

장시간 원격제어 작업중에도 빠른 속도를 유지하여 업무 효율을 높일 수 있으며 RemoteView 원격제어 소프트웨어와 연동되어 원격으로 안전하게 사용할 수 있습니다.



RemoteView BOX의 특징점



설치없이 연결하는
원격제어



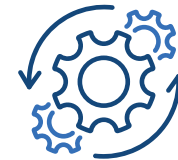
4K 고화질도
끊김없는 원격제어



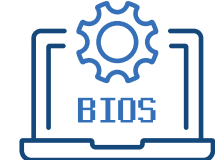
안전한 녹화
/ 접속차단



원격관리 화면에서
실시간 모니터링



노후화 OS 및
특수장비 제어



CMOS 셋업,
부팅화면 원격제어

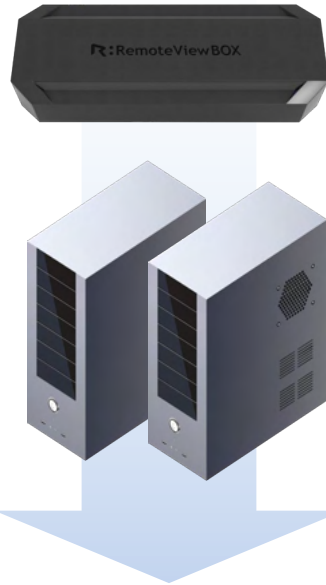
RemoteView BOX 활용 사례

RemoteWOL 제품으로 전원이 꺼져 있는 컴퓨터나 서버의 전원을 켜야 할 때 전원 제어를 할 수 있습니다.



공정 생산 라인 시스템 원격 제어

RemoteViewBOX는 공정 생산 라인 자동화 시스템 장치를 소프트웨어 설치 없이 원격으로 제어,운영,관리를 합니다.



서버 원격 모니터링, 점검, 패치 등 관리

RemoteView BOX는 IDC, 내외부망에 있는 서버를 24시간 모니터링하며 실시간으로 녹화를 할 수 있습니다.



BIOS 원격제어 가능

설비, 계측 장비의 BIOS 업데이트 및 설정을 현장 기기에 가지 않고 자리에서 손쉽게 원격으로 작업이 가능합니다.

생산망 보안 원격제어

적용 산업군 : 금융/공공/민수 등 전 분야



Pain Point

- 설비 조작을 위한 공장 내 업무 처리가 어려움
(위험, 먼 이동 거리, 작업이 어렵고 오래 걸림)
- 사용하는 원격은 보안이 취약(RDP, VNC, Radmin)하고 관리가 불가능함
- 누가, 언제, 어디서, 어떤 작업을 했는지 전혀 알지를 못함

도입 효과

- ≡ 원격 처리를 통한 업무 생산성 향상 및 인건비 절감
- ≡ 원격사용자 중앙 관리/통제로 보안사고 예방
- ≡ RVBOX로 기존에 원격제어가 불가능한 장비등이 가능해짐
(Linux, Unix, 네트워크가 없는 PC, 제조사 보안 단말 등..)

재택/원격근무/긴급장애 대응

적용 산업군 : 금융/공공/민수 등 전 분야

NH농협은행

kakaobank

MIRAE ASSET
미래에셋증권

NH투자증권

KB 증권

true friend 한국투자 증권

키움증권

신한투자증권

KYOBO 교보생명

eBEST

금융감독원
FINANCIAL SUPERVISORY SERVICE

금융보안원
FINANCIAL SECURITY INSTITUTE

금융결제원

상상인저축은행

대신증권
Daeshin Securities

롯데캐피탈

Pain Point

- 다양한 형태의 원격근무(사내업무형태가 아님) 요구 증대
- 보안, 업무 생산성, 관리감독 방안이 필요함
- VDI 방식의 도입 및 운영비용 증가(2.5배 이상)
- 감독기관의 규정을 만족하는 복잡한 시스템 필요

도입 효과

- ≡ 빠르고 간편하게 원격근무 환경 구축
- ≡ 원격근무를 위한 환경구성(전용 단말, 시스템 등) 최소화
- ≡ 자신의 업무 PC를 동일하게 사용하여 업무 연속성 보장
- ≡ 접속 권한관리 및 화면유출방지를 통한 보안성 충족

도입사례 # RemoteView BOX

SW Agent를 설치할 수 없는 장비에 RemoteView BOX로 연결한 사례

설치형 에이전트 적용이 불가능한 제약 공정 장비에 대하여 RemoteView Box와 카메라를 연동하여 장비 화면 및 상태를 원격으로 제어 및 확인 관리가 가능한 환경을 제공했습니다.

연구소 A

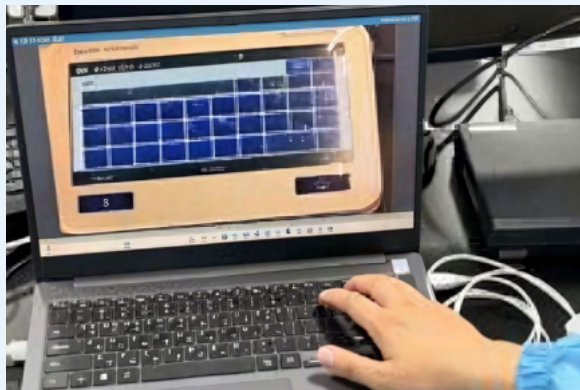
RemoteView Box
설치된 분석 키트



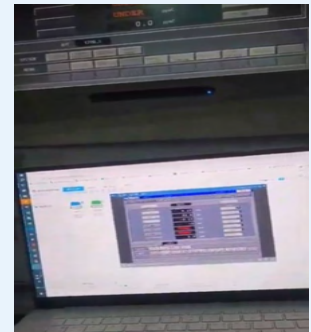
화면 공유 / 원격 제어

공장 B

연구원이 원격 접속하여
실시간 제어



선박 제조회사의 이산화탄소 측정 장비에 RemoteView Box를 연동하여, 멀리 떨어진 사무실에서도 실시간 원격 확인이 가능



도입사례 # RemoteView BOX

제약회사 공정라인 장비에 RemoteView BOX로 모니터링 환경을 구축한 사례

작업자가 직접 클린 룸에 들어가는 불필요한 리소스를 최소화 하고 클린룸 외부에서도 장비 상태를 모니터링하고 화면을 실시간으로 확인하며, 필요한 조작까지 RemoteView BOX를 통하여 수행할 수 있습니다.



기대 효과

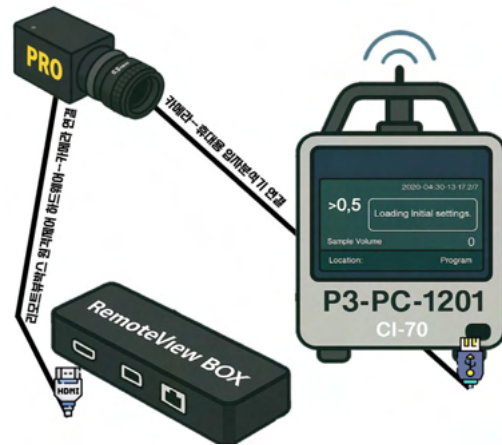
클린룸 운영에 드는 시간적·비용적 비효율성, 데이터 수집의 제약, 운영 중 오염 리스크를 기술적으로 해소하며, 기존에는 검사 종료 후 데이터만 확인하던 방식에서, 진행 중인 테스트 과정을 실시간으로 파악하고 조치를 취할 수 있는 운영 구조로의 전환이 가능하며, GMP(Good Manufacturing Practice) 규정에 위배되지 않은 안전한 약품 제조 가능

도입사례 # RemoteView BOX

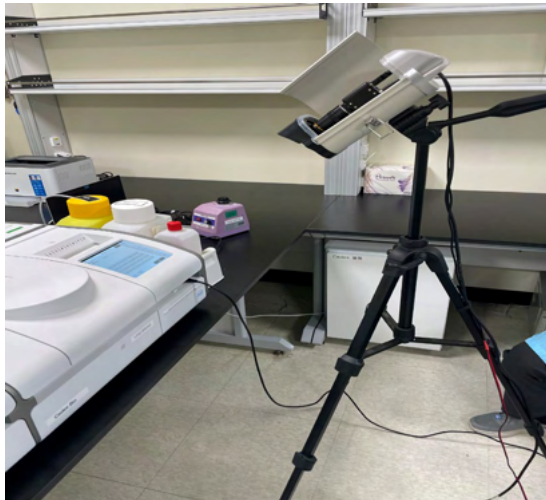
제약회사 공정라인 장비에 RemoteView BOX로 모니터링 환경을 구축한 사례

작업자가 직접 클린 룸에 들어가는 불필요한 리소스를 최소화 하고 클린룸 외부에서도 장비 상태를 모니터링하고 화면을 실시간으로 확인하며, 필요한 조작까지 RemoteView BOX를 통하여 수행할 수 있습니다.

제약 회사 실제 구축 사진



RVBOX↔검사기기 연결방법



실제 연결 모습



다양한 장비 연결 가능

다수의 기업이 선택한 RemoteView OT 솔루션

150명 이상의 R&D 전문 인력의 끊임없는 기술 인프라로 RemoteView OT는 여러 기업들과 함께하고 있습니다.



공장 설비 원격제어 솔루션, RemoteView OT 지금 바로 문의하세요.

전화 문의 : 070-7011-3900

구매 문의 : sales.kr@rsupport.com

Korea

05203 서울시 강동구 고덕밸리로2가길 12 (고덕동)
전화 : +82-70-7011-3900
팩스 : +82-2-479-4429
기술 문의 : support.kr@rsupport.com
구매 문의 : sales.kr@rsupport.com

Japan

東京都港区東新橋2-3-3 ルオーゴ汐留
10階ご購入前のご相談 : 03-6273-3871
テクニカルサポート : 03-6273-3872
お問い合わせ : <https://help.remotecall.com>

China

北京市朝阳区阜通东大街6号方恒国际A座2708
咨询电话 : +86-10-8256-1810
联系邮箱 : co-china@rsupport.com