

iPScan[®] NAC

Network Access Control

통합 네트워크 접근제어 솔루션

네트워크 접근제어 | IP관리

사용자 인증 | 단말 인증 | S/W관리 | 패치관리

Mobile 제어 | WiFi AP제어 | CCTV 통제 | PLM | 원격제어

스마트 시티 | 스마트 팩토리 | IT보안 | OT보안 | IoT보안

IPScan[®] NAC

고객맞춤형 통합 네트워크 접근제어 솔루션

IPScan NAC (Network Access Control)은

고객의 내부 정보보안체계를 수립하여, 유·무선 네트워크에 접속되는 모든 사용자와 디바이스의 접속을 제어/통제하여 내부 정보 유출을 막고, 애플리케이션을 신속, 안전하게 작동할 수 있도록 각 디바이스의 취약점을 보완, 관리하는 **네트워크 접근제어 솔루션**입니다.

▶ 필요성 Needs

▷ 급증하는 IoT보안 위협

클라우드, IoT, BYOD, 엣지컴퓨팅, 환경에서 내부 유·무선 네트워크에 무제한 연결되는 엔드포인트 증가로 무차별 공격에 노출

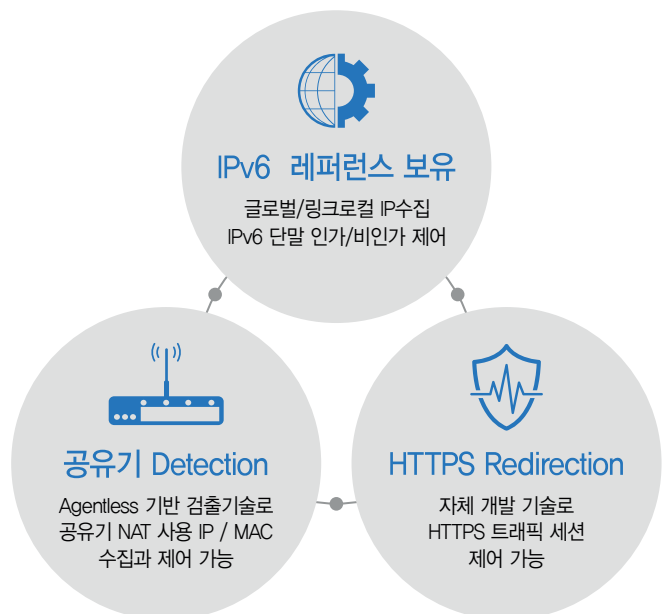
IoT 기기는 보안에 취약한 어플리케이션을 사용하여 기업 내부의 민감한 데이터가 외부에 노출되기 쉬운 구조로 보안 위협의 원천적인 해결 필요성 증대

▷ Zero-Trust 보안 확대

정보보호 대상이 시스템 중심에서 데이터, 사용자, 워크로드 등 사용자 중심의 'Zero-Trust' 보안 모델로의 전환 필요

비즈니스 결과 중심, 보호 자산과 데이터를 바탕으로한 내부 설계, 최소 접근 권한 기반 사용자 접근 범위 결정, 모든 트래픽 검사와 로그 기록을 위해 네트워크 접근 제어 솔루션 필요성 증대

▶ 핵심 기능 Core Functions



▶ 주요 적용 분야 Major Application Field

iPScan NAC
통합 네트워크 접근제어 솔루션



유·무선 네트워크 보안

- Agent/Agentless 기반 IP/MAC 주소 자동탐지
- 인가/비인가 단말 네트워크 접근 제어
- 단말 무결성 확인과 취약점 제거 가이드
- OS 탐지와 단말 유형별 식별
- 조직/개인 단위 모니터링과 통제



CCTV 보안

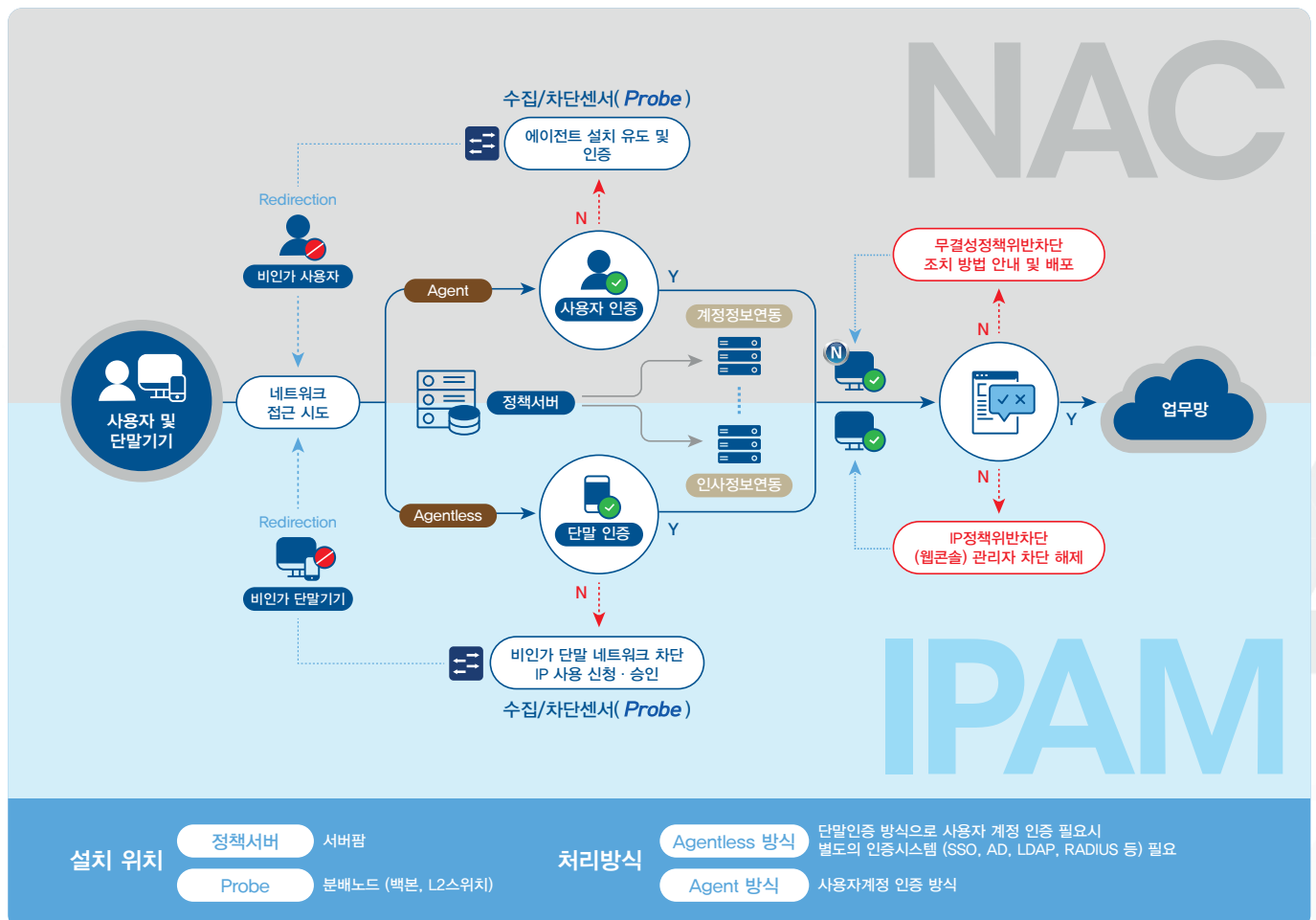
- CCTV 제어 트래픽 모니터링
- CCTV ON/OFF 상태 확인
- CCTV 네트워크 차단과 트래픽 제어
- 비인가 사용자 VMS 접근제어



산업 IoT 보안

- 산업용 IoT GW 장비 제어
- GW 네트워크 비인가 단말 접근 통제 및 모니터링
- IoT장비와의 결합형 자산관리
- 원격전원제어를 통한 비상대응(오프선)

▶ 솔루션 개념도 Solution Concept



▶ 주요 기능 Major Functions



네트워크 탐지 및 통제

- PC, 모바일 단말, 서버, CCTV 등 IT자산 자동 탐지
- IP/MAC 변경, 충돌 장애 방지, 우회 통신 경로 방지 등
- 인사정보 연동을 통한 사용자 구분 기능
- 사용 용도에 맞는 단말기 구분 기능
- 사내 보안 정책 준수를 위한 네트워크 통제 정책 지원



단말 무결성 검증

- Nom-Drive 기반의 Agent로 독립성 보장
- 단말 SW무결성을 위한 단말 정보 수집
- 필수/악성 소프트웨어 검사 및 제어
- Windows 보안 업데이트 검사 및 제어



사용자 인증

- Agent를 통한 ID/Password 사용자 인증 및 인증 개수 제한
- IP대역 내 별도 구역 설정을 통한 IP사용 대역 제어
- AD, LDAP, SSO 등 통합 인증 연동 및 계정 승인
- RDBMS 및 CSV등 다양한 포맷의 연동 API 지원



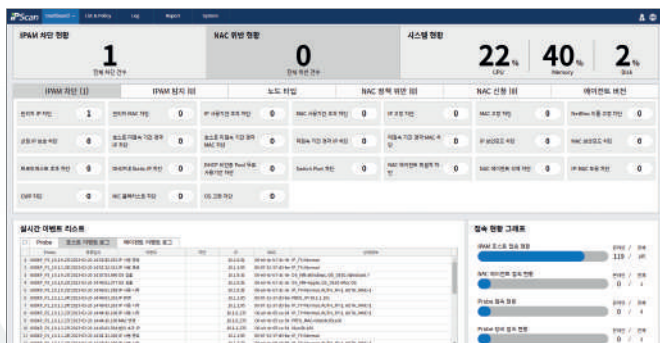
관리 기능

- IP/MAC 사용시간, 차단 현황 및 사유 관리
- 필수 SW 및 패치 관리 기능
- 주기별 패치 검사 및 상태 정보 제공
- 관리 편의를 위한 사용자, IT자산 자동 분류 기능

▶ 관리자 화면 Web UIX

보안관리자 인터페이스 제공

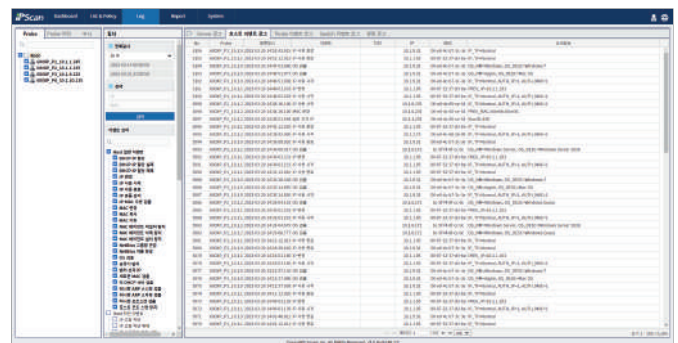
- 대시보드, 네트워크 사용 현황, 관리 로그, 시스템 정보 제공
- 조직도 및 IP 기반 관리로 효율적인 운영 가능



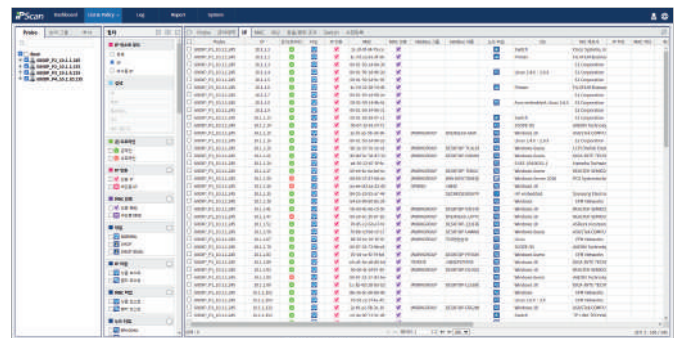
사용자 편의를 고려한 직관적인 UIX제공



사용자 인증 및 무결성 검증 확인



IP/MAC 관리 / 네트워크 현황



이벤트 로그관리 및 통제

▶ **특장점** Key Features



네트워크 위험요소 사전 제어

- 네트워크 접속 사용자 및 단말 중앙 통합관리
- 고객사 환경에 맞춘 인증 정책과 계정 관리
- 사내 보안 정책 인증과 보안 규제 준수



Agent / Agentless 혼합 구성

- 탄력적인 NAC 정책 운용 가능
- 센서 장비를 통한 네트워크 접근 통제
- 폭 넓은 네트워크 접근제어 범위 제공



IPv6 지원을 통한 IoT 기기 제어

- IPv6를 관리 범위에 포함하여 다기종 IoT 단말 제어
- 사용자 편의성 보장 위한 체계적인 보안 체계 구축



다양한 분석, 보고서 제공

- 풍부한 현장 경험에 근거한 세밀한 운영 현황 분석
- Drill-down 방식을 적용한 점층적 로그 분석
- 내·외부 감사 위한 네트워크 이력 보고서 제공



네트워크 환경에 영향이 없는 간단한 설치

- 네트워크 구조 변경 없이 단순 추가 설치 구축
- 사용 환경에 따라 에이전트 설치 여부 선택 가능
- 3rd Party와의 유기적 연동으로 인프라 활용 극대화



On-Demand 구성

- 모듈 방식으로 정책서버 1대로 IP관리, NAC 가능, 비용 절감
- 1개의 Web콘솔로 IP관리, NAC 관리가 가능, 관리자 편리성 증대

▶ **제품 구성** Product Composition

| | 정책서버 (Server) | 수집 차단센서 (Probe) | 에이전트 (Agent) |
|----------|--|--|--|
| 주요 기능 | <ul style="list-style-type: none"> • 사용자 네트워크 접속 통제 및 보안 정책 관리 및 감사 • 보안정책 DB 및 감사 로그 관리 • IP관리 및 NAC 통합 정책서버 | <ul style="list-style-type: none"> • 모든 단말 IP/MAC정보 수집 및 모니터링 • 네트워크 차단/허용 정책 수행 • DHCP IP할당 | <ul style="list-style-type: none"> • 사용자 단말 관리, 통제 • 필수SW 설치유도 및 보안설정 강제 |
| Type | <ul style="list-style-type: none"> • IPScan NAC 500+ • IPScan NAC 1000+ • IPScan NAC 2000+ • IPScan NAC 10000+ | <ul style="list-style-type: none"> • IPScan Probe 50X+ • IPScan Probe 100X+/100X+4port • IPScan Probe 200X+/200X+4port • IPScan Probe 400X+ • IPScan Probe 600X+ • IPScan Probe 1000X+ • IPScan NAC RPM Probe 100X+ 5port | <ul style="list-style-type: none"> • IPScan NAC Agent |

▶ **고객 맞춤형 솔루션** On-Demand Solution 고객 요구에 따라 맞춤형 통합 솔루션 제공





iPScan[®] NÄC

www.scope.co.kr

스콧정보통신



(06716) 서울시 서초구 반포대로 10길 24(서초동, 차영빌딩)
Tel. 02-3412-9700 / Fax. 02-3412-9800

제품문의 : sales@scope.co.kr
기술지원 : 02-2084-8282 / sos@scope.co.kr

Copyright Scope Inc. All Rights Reserved.

INNOBIZ
기술혁신명중소기업

MAIN Biz
경영혁신명 중소기업