Tgate 시스템 소개

The True Concept of Network Access Control





CONTENTS

01 회사 소개

NAC 필요성 02

03 주요 기능

추가 기능 04

05 특강점

인증서 06

07 구축 사례

레퍼런스 08



회사 소개

회사소개

㈜엠엘소프트는 1995년 설립된 Endpoint 관리 및 통제를 전문으로 연구개발하고 있습니다.
TCO (Total Cost Ownership) 컨셉트를 국내에 성공적으로 소개하고 DMS(데스크톱통합관리솔루션) 시장을 선도하였으며,
20년간 집중해 온 엔드포인트 기술력을 바탕으로 2006년부터 네트워크 접근통제 시스템(NAC, Network Access Control)인 티게이트(Tgate)를 출시하여 NAC 시장을 주도하고있습니다.

MLsoft
Pioneer of Endpoint Management

❖ 기업 주요 내용

설립연도: 1995년

사업분야: 엔드포인트 관리 및 통제 전문 개발

주요제품: DMS(PC자산관리), PMS(Patch 관리), IPM(IP관리), NAC(네트워크접근통제)

인원분포: 전 직원의 85%가 기술 인력 (연구개발 주력 기업)

❖ Tgate 수상 내역

2015 대한민국소프트웨어대상 미래창조과학부 장관상 수상

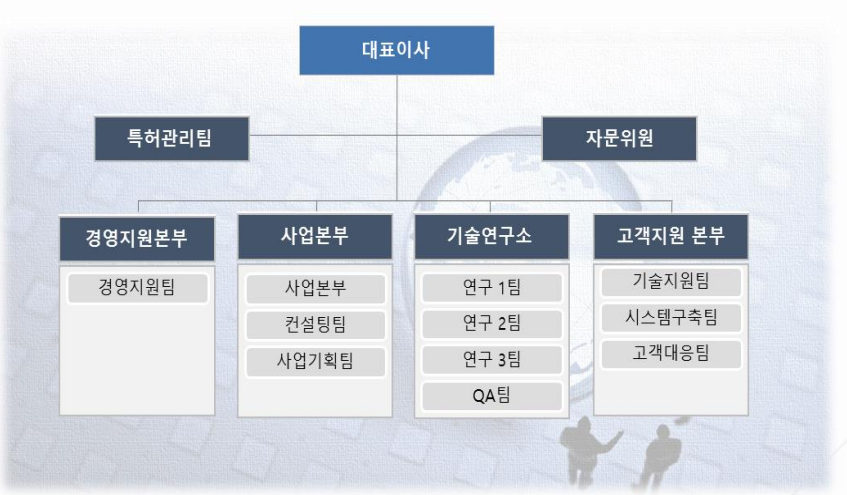
2015 하이테크어워드 보안솔루션 부분 수상

2014~2015 DT 브랜드파워 대상 수상

2013~2014 보안솔루션 부문 품질우수 히트상품 수상(디지털타임즈)

2011 한국을빛낸대표브랜드 IT서비스(보안솔루션) 부문 大賞 수상







NAC 필요성

NAC 필요성

여러 형태의 경로를 통하여 사내 네트워크 접속하는 단말에 대하여 네트워크를 모니터링하고
위험을 발생 시키는 단말과 인증되지 않은 사용자의 접근을 차단해야 하는 필요성이 대두

보안 사고는 보안 패치가 발표된 이후 공격자들은 빠르게 움직여 시스템의 약점을 파악하여 악성 코드를 만들어 여러가지 방법으로 Endpoint를 공격합니다.
반면 기업의 보안 담당자들은 패치 발표 이후 여러가지 방법으로 패치를 진행하지만 마지막 PC까지 모두 보안 패치를 설치하기 까지는 상당한 시일이 걸립니다.
또한, 패치가 다 이루어지기 전에 다른 악성 코드가 유포되고 있는 시점입니다.

이러한 피해를 줄이기 위해 기업들은 인증되고 검역이 된 단말만 내부 망으로 허용하고,
미확인된 단말들은 내부 망과 단절 시킬 수 있어야하며, 미확인된 단말을 차단하고, 스캔할 수 있어야 합니다.
따라서 단말을 완벽하게 내부로 접근 할 수 없도록 하면서, 사용자 확인 및 패치 검사와 시스템 검역을 통하여 안전한 상태인지를 확인 후 내부 망 접속을 허용 할 수 있는 시스템이 필요하게 되었습니다.

NAC는 오염된 기기들이 내부 망에 접근 할 수 없도록 내부망을 안전하게 지키는 역할을 합니다.
NAC의 필수 요소는 상황에 맞는 모니터링과 격리에 있습니다.

따라서 NAC에서는 내부 망 접속 전, 후 관리 체계를 강화하여 사전에 대응하고 예방 할 수 있도록 Endpoint에 검역을 실시하여 취약성을 예방하고 이상 행위 발생 시 내부 망에서 격리합니다.

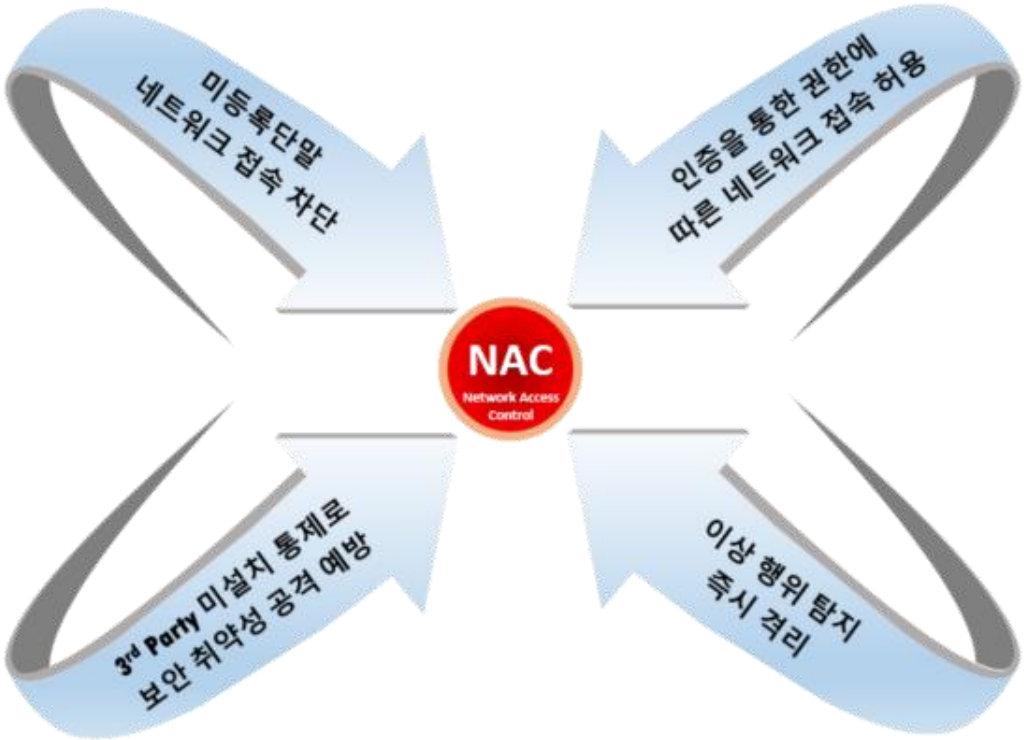
- Network에 접속하는 모든 유형단말의 현황파악 및 제어, 차단, 보호, 승인
- 허가된 장비만 접속(승인)하며, 등록된 사용자만 접속(인증)
- 단말 무결성 체크, 네트워크 전체를 clean하게, 3rd SW 100% 설치 상태로
- Role에 따른 네트워크 접근제한 (ex. 내부직원/외부직원/Guest)
- 보안 Level 지속 유지, 이상행위 탐지
- 네트워크에서 발생되는 모든 이력 탐지 및 기록



NAC 필요성

여러 형태의 경로를 통하여 사내 네트워크 접속하는 단말에 대하여 네트워크를 모니터링하고
위험을 발생 시키는 단말과 인증되지 않은 사용자의 접근을 차단해야 하는 필요성이 대두

내부 망에 접속하는 단말의 보안 상태를 확인 할 수 있는 시스템 및 이력 관리 부재로 악성 감염 단말에 대한 파악의 어려움
(취약성에 노출)



내부에 단말을 모든 인력이 사용할 수 있는 상태로 자료 유출 및 내부 시스템 접속 가능성
(네트워크 취약성)

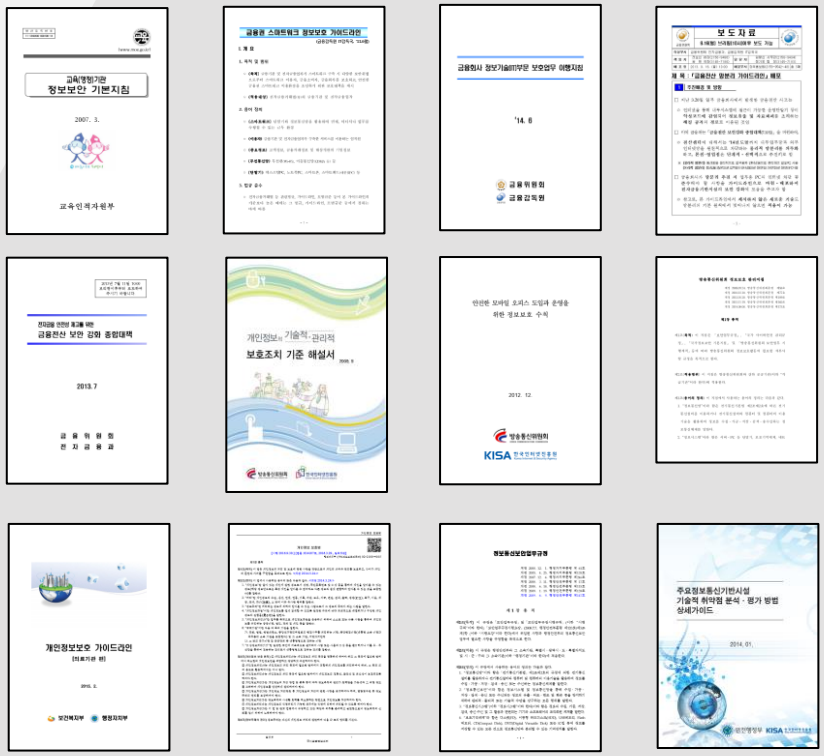
3rd Party 솔루션의 미설치 PC 처리 방법 부재와 미설치로 인한 보안 취약성 공격에 노출
(바이러스 등의 감염)

단말의 이상 행위 발생에 대한 인지 및 행위에 대한 감시 부재
(네트워크 취약성)

NAC 필요성

보안규정 시행 강화 (기업/기관의 내부 보안에 대한 적절한 보호조치 요구)

- (교육부) 정보보안기본지침
- (금융감독원)금융권 스마트워크 정보보호 가이드라인
- (금융감독원 /금융위원회)금융회사 정보기술(IT)부문 보호업무 모범규준
- (금융위원회) 금융전산 망분리 가이드라인
- (금융위원회) 금융전산 보안 강화 종합대책
- (방송통신위원회)정보보호 관리지침
- (방송통신위원회)모바일 오피스 정보보호수칙
- (방송통신위원회)개인정보의 기술적, 관리적 보호조치 기준
- (보건복지부)의료기관 개인정보보호 가이드라인
- (안전행정부)개인정보보호법
- (안전행정부)정보통신 보안업무규정
- (안전행정부) 주요정보통신기반시설 기술적 취약 분석 평가방법 상세 가이드



MLsoft
Pioneer of Endpoint Management



Tgate 주요기능

NAC 필수 요소

네트워크에 접근 하는 모든 단말의 모니터링과 네트워크 접근 전, 후에 따라 수행해야 할 기능 요소



유선 엔드포인트 인증

유선으로 연결된 노트북, 데스크탑PC, 프린터, 인터넷전화기 등 모든 유선 엔드포인트를 탐지, 인증 합니다.



무선 엔드포인트 인증

안드로이드폰, 아이폰, 아이패드 등 무선 Wi-Fi 를 통해 통신하는 모든 무선 엔드포인트를 탐지, 인증 합니다.



사용자 인증

유무선 엔드포인트로 사내 접속하려 하는 사람을 확인, 인증 합니다.
사용자 확인은 초기 1회만 할 수도 있으며, 매일 아침 재인증을 요청할 수도 있습니다



방문자 인터넷만 사용

단순히 인터넷만 사용하고자 하는 방문객에게 내부망 접속은 차단시키고
인터넷 사용권한만 주어 내부 보안과 편의성을 동시에 제공할 수 있습니다.



필수 소프트웨어 설치 / 악성 소프트웨어 제거 강제화

내부망 접근 전에, 백신과 같은 반드시 설치해야하는 보안 프로그램들은 설치를 강제화 합니다.
P2P 프로그램과 같이 악성 코드를 쉽게 유입시킬 수 있는 프로그램들은 삭제를 강제화 합니다



불법 무선 공유기 차단

회사의 허가 없이 직원들이 임의적으로 설치한 무선공유기는 보안 허점이 되어
악성 코드 유입 경로가 될 수 있습니다.
허가 없이 설치된 무선 공유기를 탐지하고 차단 할 수 있습니다.



인가 후 주기적 소프트웨어 상태 검사

내부망에 접속된 엔드포인트일지라도 주기적으로 소프트웨어 보안상태를 점검하여,
사내 보안정책을 따르지 않은(백신 프로세스 중지 등) 엔드포인트가 발견되면,
즉시 내부망에서 격리 시켜 사내 인프라를 보호 할 수 있습니다.



권한 별 보안수준 차등화 / 부서별 접근 통제

내부망에 접속된 엔드포인트일지라도 주기적으로 소프트웨어 보안상태를 점검하여,
사내 보안정책을 따르지 않은(백신 프로세스 중지 등) 엔드포인트가 발견되면,
즉시 내부망에서 격리 시켜 사내 인프라를 보호 할 수 있습니다.



이상 트래픽 발생시 자동 통신 차단

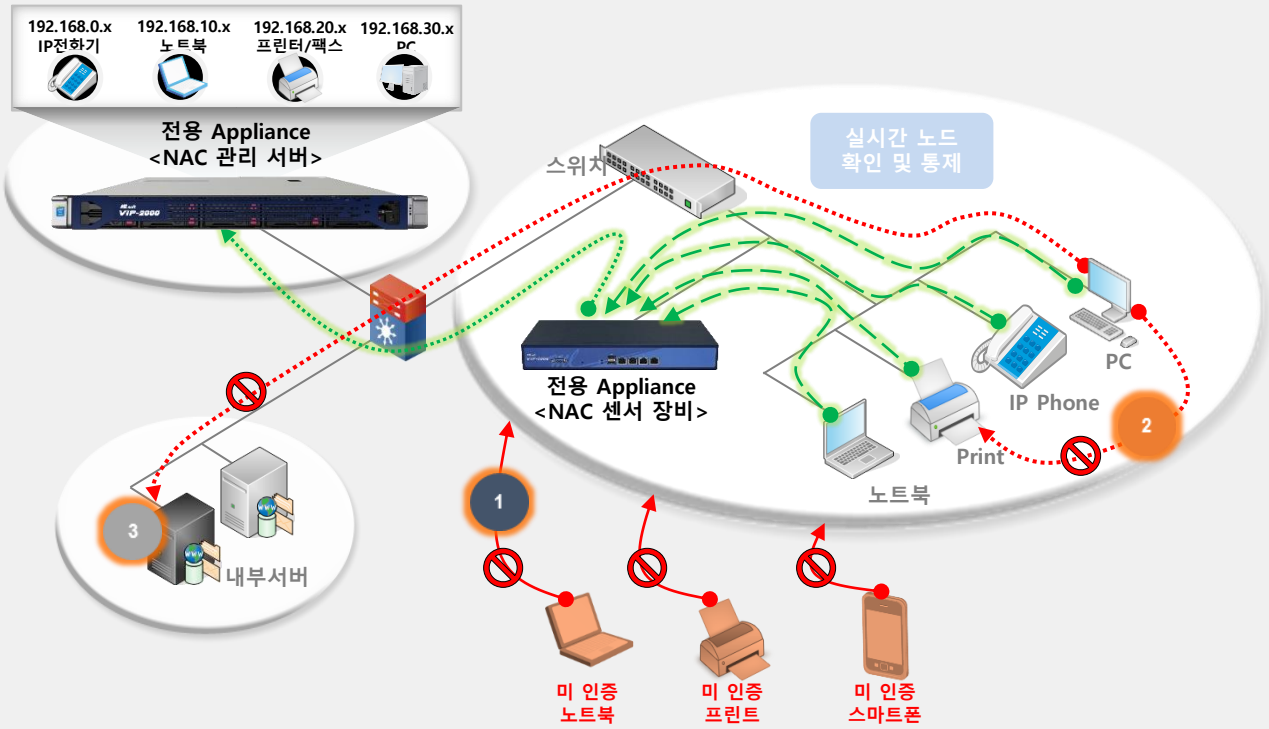
기준치 이상의 트래픽을 발생 시키는 PC발견시, 즉시 통신을 차단 시켜 내부망에서 격리 시킵니다.

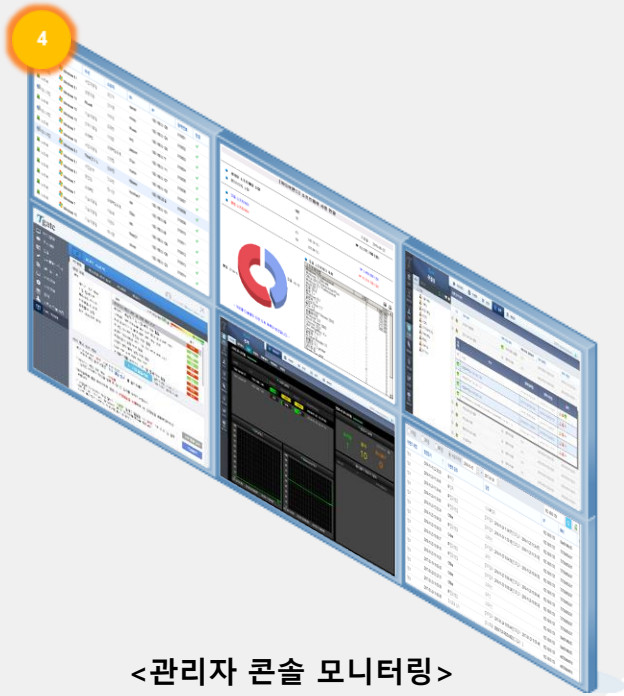
Agentless 기반 접근 통제

모든 단말에 대한 감지, 인가 및 차단, 사용자 인증, 이력 및 추적관리

Agent 설치없이 네트워크에 접속하는 모든 유형의 단말을 통제하고 Web GUI 를 통한 인증 및 강력한 네트워크 통제 기술을 통하여 IP 대역 및 그룹간 네트워크 접근 제어를 수행합니다.

1. 단말의 IP/MAC 네트워크 접근 통제
2. 사용자 인증 및 권한에 따른 접근 통제
3. Port 및 Protocol별 네트워크 접근 통제
4. 관리자 콘솔을 통한 모니터링





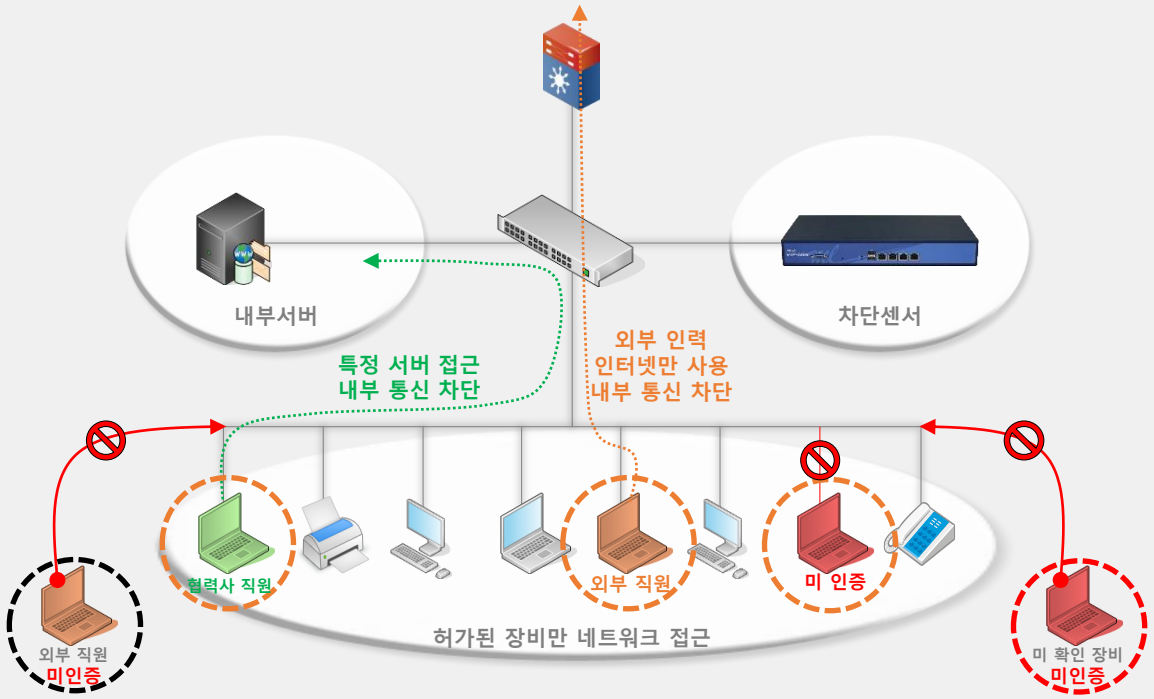
<관리자 콘솔 모니터링>

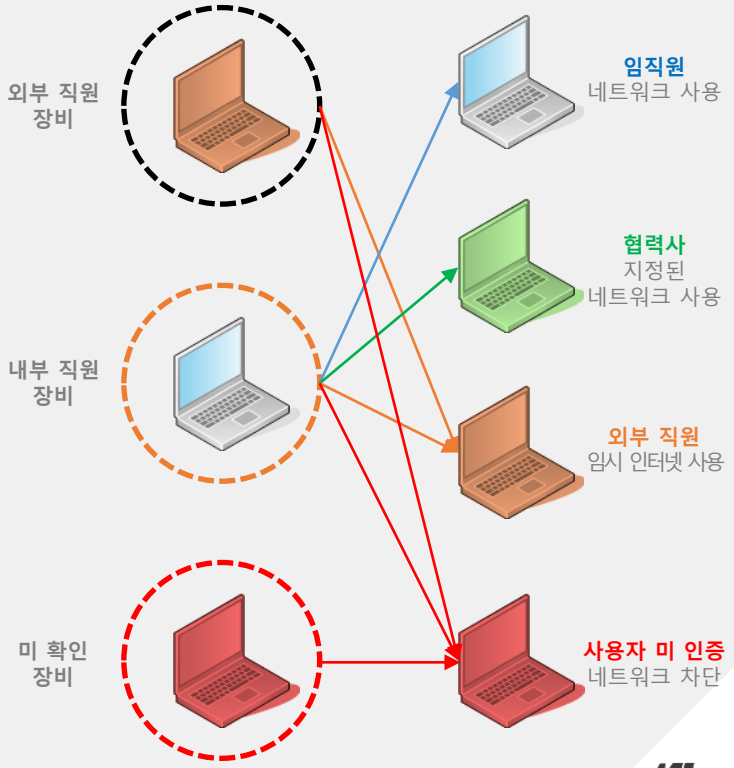
장비 및 사용자 인증

허가 장비 외 모든 단말에 대한 통제 관리 및 사용자 인증에 따른 권한 부여

네트워크에 접근하는 모든 단말에 대하여 장비 인증을 받아 신뢰 할 수 있는 네트워크 환경을 구축하며, 사용자 인증에 따른 네트워크 접근 통제로 Role에 따라 임직원, 협력사, 외부직원, 공용PC 등의 접속 권한을 제어 할 수 있습니다.

1. 허가된 단말만 네트워크에 접속
2. 사용자 로그인을 통한 네트워크 차등 관리
3. 미 확인 단말의 통제 관리
4. 방문객을 위한 임시 인터넷 기능 지원



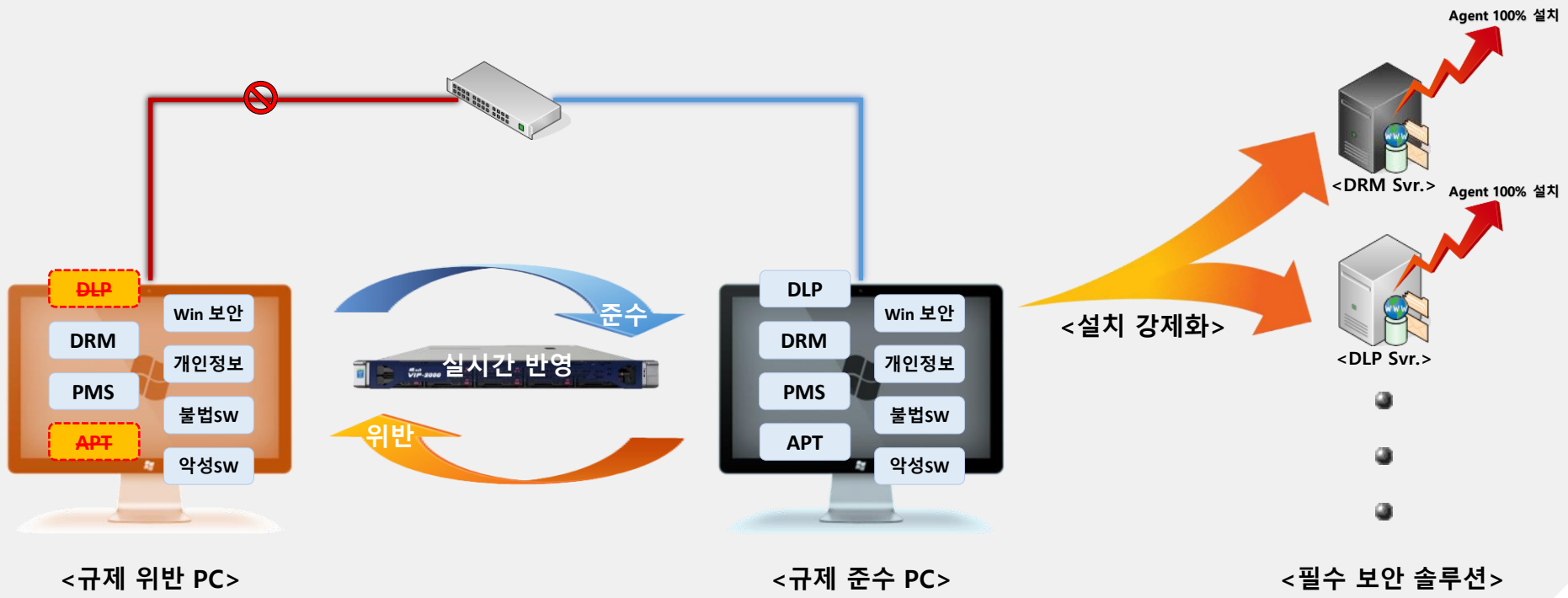


PC 무결성 검사

실시간 PC 무결성 검사를 통해 사내 필수 소프트웨어 관리하여 보안 취약성 사전 예방

PC 무결성 검사를 통하여 단말의 취약성을 사전에 예방하며, 3rd Party 제품의 Agent 설치를 100%로 유지할 수 있도록 강제화 합니다. 또한, 내부/외부/공용/기타 사용자 정보를 구성하여 타 시스템에 통합 인사 데이터를 제공합니다.

1. 사용자 PC 보안 상태 확인 및 통제
2. 필수SW 설치 강제화 (3rd Party 설치 운영 100% 유지)
3. Windows 보안 상태 유지 관리 및 Windows 업데이트 자동 설치
4. 사용자 규제 위반 시 실시간 알림 및 통제

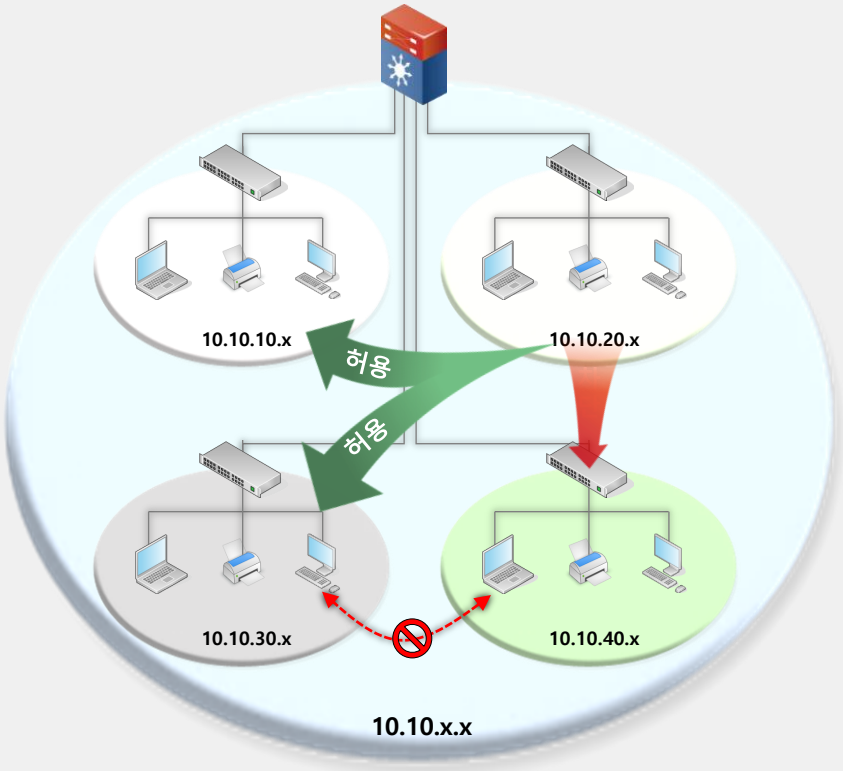


Role-base 권한 설정

사용자 로그인 권한별 네트워크 관리 및 접근 통제

사용자의 로그인 계정에 따라 전체/부서/개인별 Role 정책을 부여하여 관리자가 지정한 정책에 의하여 IP 방화벽 역할을 수행합니다. 또한, IP의 대역 간 통신 제어 기술을 이용하여 네트워크 접근 제어를 수행합니다.

1. IP 대역별 네트워크 접속 통제 (IP base)
2. 내/외부, 방문객 등의 권한에 따른 네트워크 접속 통제 (계정 base)
3. Agent-less 네트워크 통제 수행 (차단 센서)
4. Agent 에서 네트워크 통제 수행 (NAC Agent)



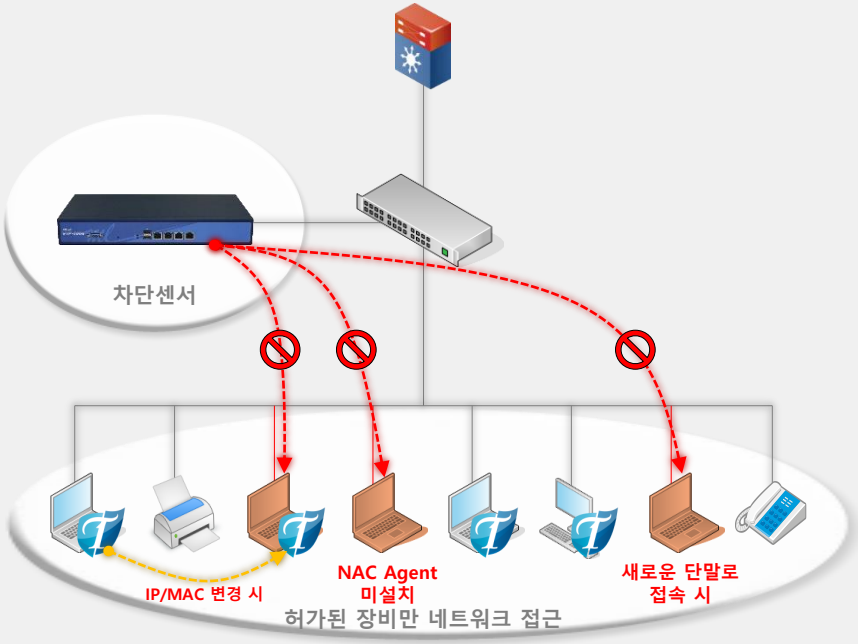


이상 행위 탐지

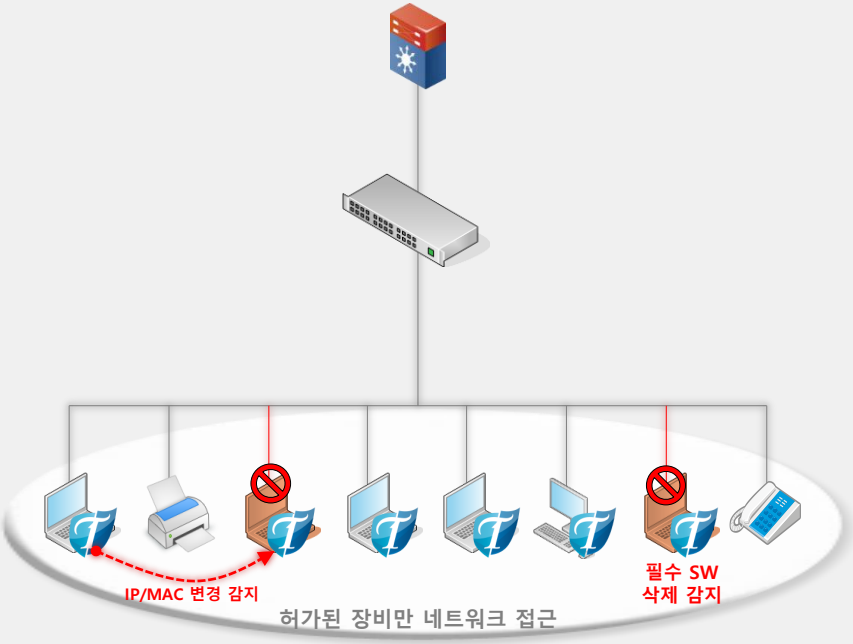
단말 및 네트워크 이상 행위 탐지 시 통제

차단 센서의 감지 기술을 통하여 네트워크에서 발생되는 위/변조 및 IP 변경을 모니터링하여 이상 행위 탐지 시 정책에 의해 즉시 네트워크를 통제합니다.
NAC Agent 또한 위/변조와 IP 변경, 규제 위반 단말의 네트워크를 통제합니다.

1. 네트워크 변경 감지 시 통제
2. Agent 미설치 통제 (차단센서)
3. PC의 IP/MAC 변조 및 변경 감지 통제
4. PC의 무결성 위반 시 통제 (Agent 기능)



<NAC 차단센서 역할>



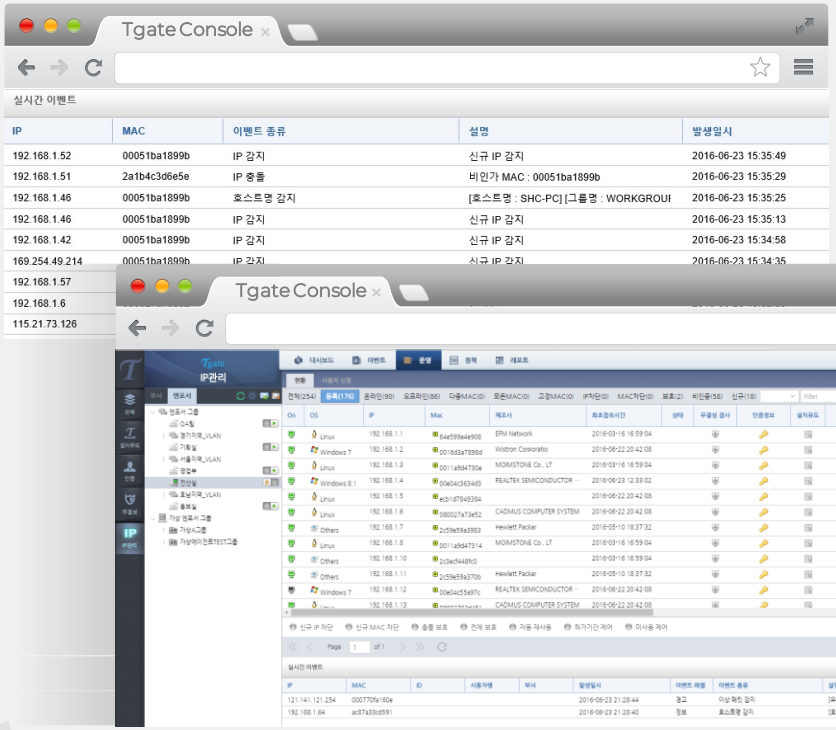
<NAC Agent 역할>

통계 및 레포트

단말의 IP/MAC 이력 및 사용자 이력, 실시간 위협 탐지에 대한 관리

네트워크에서 발생되는 모든 신호를 실시간으로 기록하고 ARP 임계치 등 위협 탐지 시 관리자에게 알림하여 네트워크 보안 사고를 사전에 예방합니다.
모든 이력에 대하여 통계 및 추적이 가능하도록 Log 이벤트를 제공합니다.

1. IP/MAC 실시간 이력 관리
2. Agent 설치 대상 PC의 이력 관리
3. 사용자 무결성 및 실시간 위협 탐지 이력 관리
4. 사용자 무결성 및 실시간 위협 탐지 이력 관리









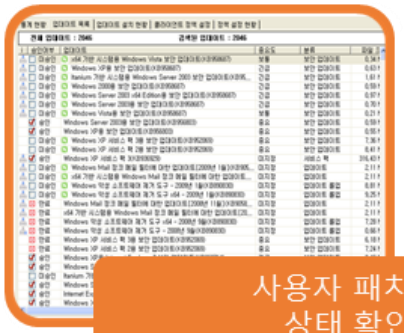
Tgate 추가기능

패치관리

Windows OS 패치 이력 관리 및 자동 배포

패치 상태 확인

백그라운드에서 정해진 시간에
맞춰 자동으로 패치 검색



사용자 패치
상태 확인

패치 정책 수립

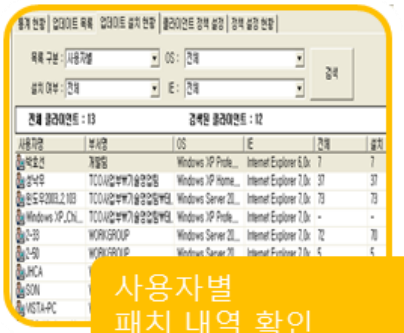
사내 전체 / 부서 / 개인별
정책 수립



패치 정책
설정

패치 내역 확인

전체 / 부서 / 개인별
패치 내역 상세 확인



사용자별
패치 내역 확인

패치 결과 모니터링

관리자 콘솔을 통한 대시보드
패치 종류, 진행률 확인



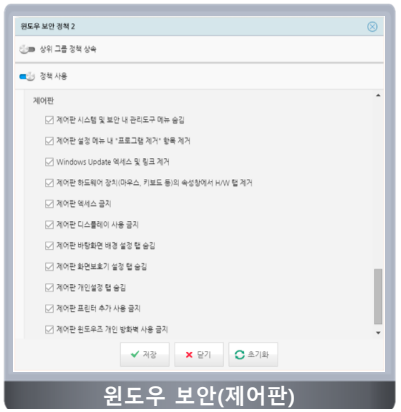
패치 상태 확인 및
모니터링

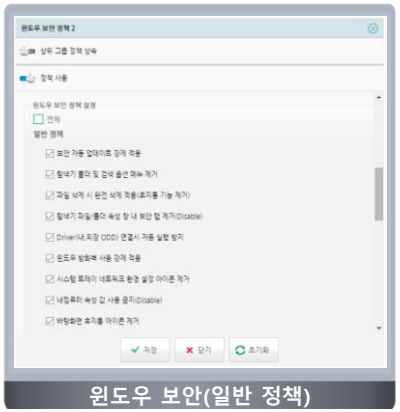
윈도우 보안

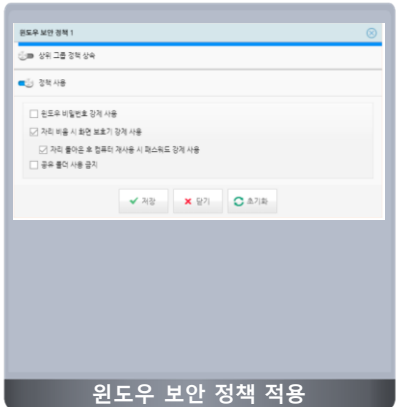
Windows 취약성에 대한 중앙 통제 및 사용자 PC 강제화

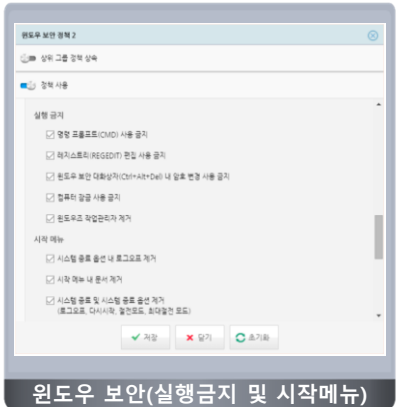
윈도우 기기 통제 기능

- 일반 정책
- 제어판 정책
- 실행 금지 정책
- 시작 메뉴 정책


윈도우 보안(제어판)


윈도우 보안(일반 정책)


윈도우 보안 정책 적용

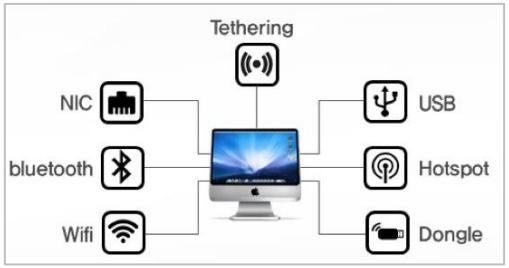

윈도우 보안(실행금지 및 시작메뉴)

우회 경로 차단

테더링, 블루투스, 무선 AP 등의 내부 통신 외 어댑터 관리 및 통제

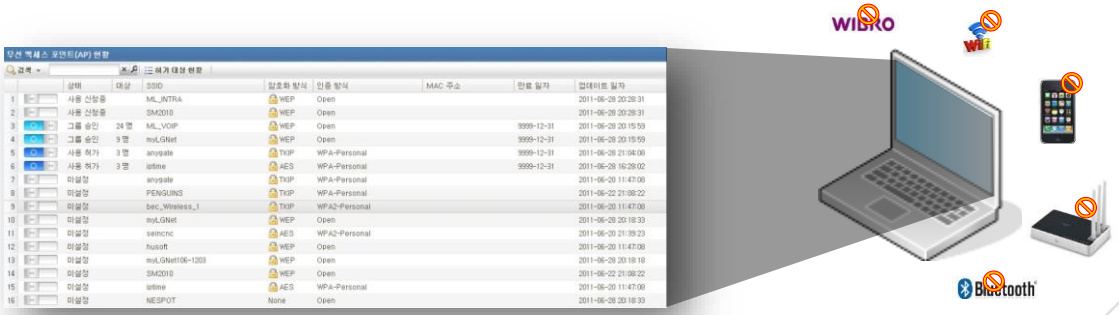
유/무선 및 모바일 기기 통제

- 스마트폰 테더링 및 AP 기능 차단
- 허가되지 않은 무선AP 접속 통제
- PC주변의 검색 가능한 무선 AP현황 모니터링
- 허가되지 않은 네트워크 어댑터 통제
  - 모바일 기기의 테더링을 통한 네트워크 접속
- 사용자PC의 네트워크 어댑터 현황 모니터링
  - 비허가 네트워크의 접속 제한 및 차단
  - 유선랜, 무선랜, 블루투스, USB, 테더링 등
  - 제어판 설정 변경 금지



서버와 연결된 어댑터 외 차단



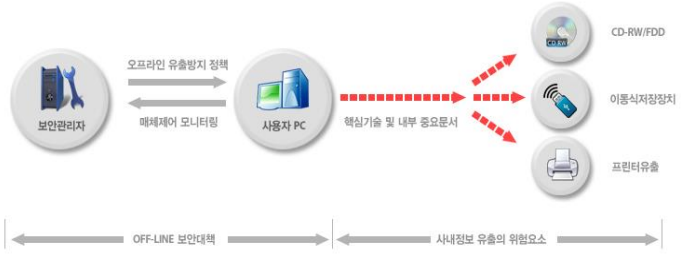


매체통제

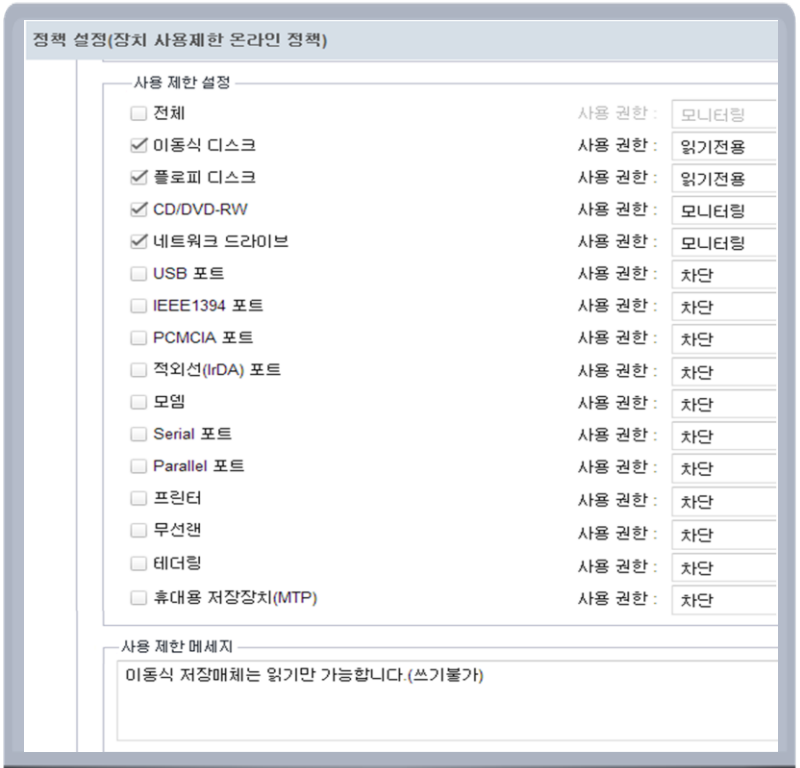
사용자 PC의 이동식 매체의 읽기/쓰기 및 USB 포트 등의 기타 매체에 대한 차단/허용

PC 저장 매체 제어

- CD-RW, FDD, USB 등을 통제 관리 함으로써 각종 내부 정보의 외부 유출 방지 지원
- 통제 범위
  - 드라이버 통제 – 이동식디스크(USB), 프린터, CD/DVD, 공유폴더 등
  - 포트 통제 – USB, Bluetooth, IEEE1394, PCMCIA, IRDA, Serial 등
  - 복합장치 제어 – Wibro, ActiveSync, FixedHDD, 무선랜, 테더링 등
- 통제 정책
  - 차단/허용 – 모든 매체에 적용 가능
  - 읽기전용/로그 – 대부분의 드라이버 방식 매체
  - 원본 저장 – USB Memory, CD-RW, 프린터



매체 제어 정책 설정



매체 정책 설정

불법 SW 통제

허가 받지 않은 불법 SW 사용에 대한 중앙 통제 및 정품 라이선스 관리

사용자 PC 불법 소프트웨어 점검

사내 정품 승인 받지 않은 소프트웨어 차단

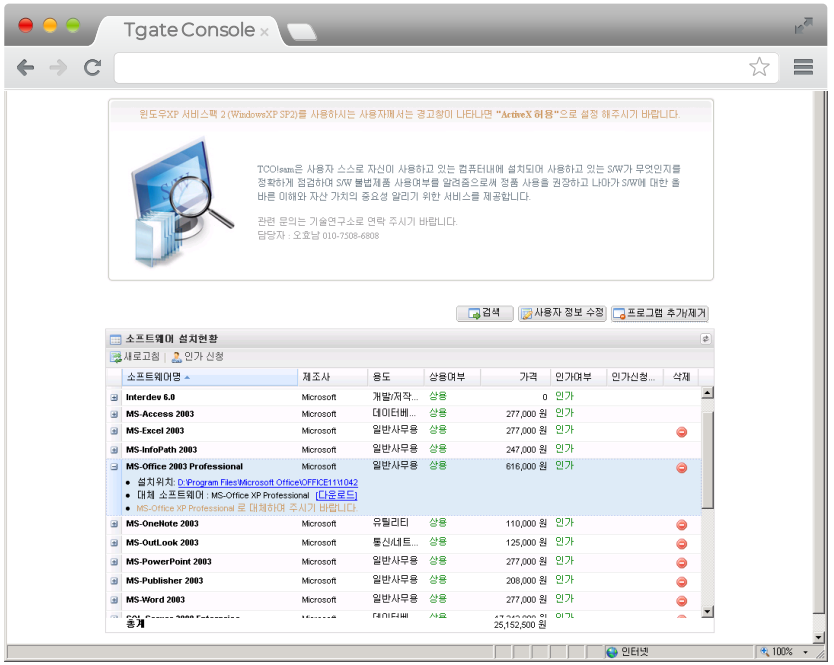
불법 SW 사용 단말 네트워크 통제

- 불법소프트웨어 탐지 시 사용자 알림
- 불법소프트웨어 차단
- 위반 시 네트워크 통제
- 위반 시 대표 SW 차단

불법 SW 삭제 유도 버튼 제공

- 강제 삭제가 아닌 사용자 권한 삭제로 PC 안전성 확보
- 차단 알림 통해 정품 소프트웨어 사용 유도

불법 SW 사용자 알림 창



원격제어

사용자 단의 Help 요청 시 담당자 PC에서 직접 사용자 PC 제어

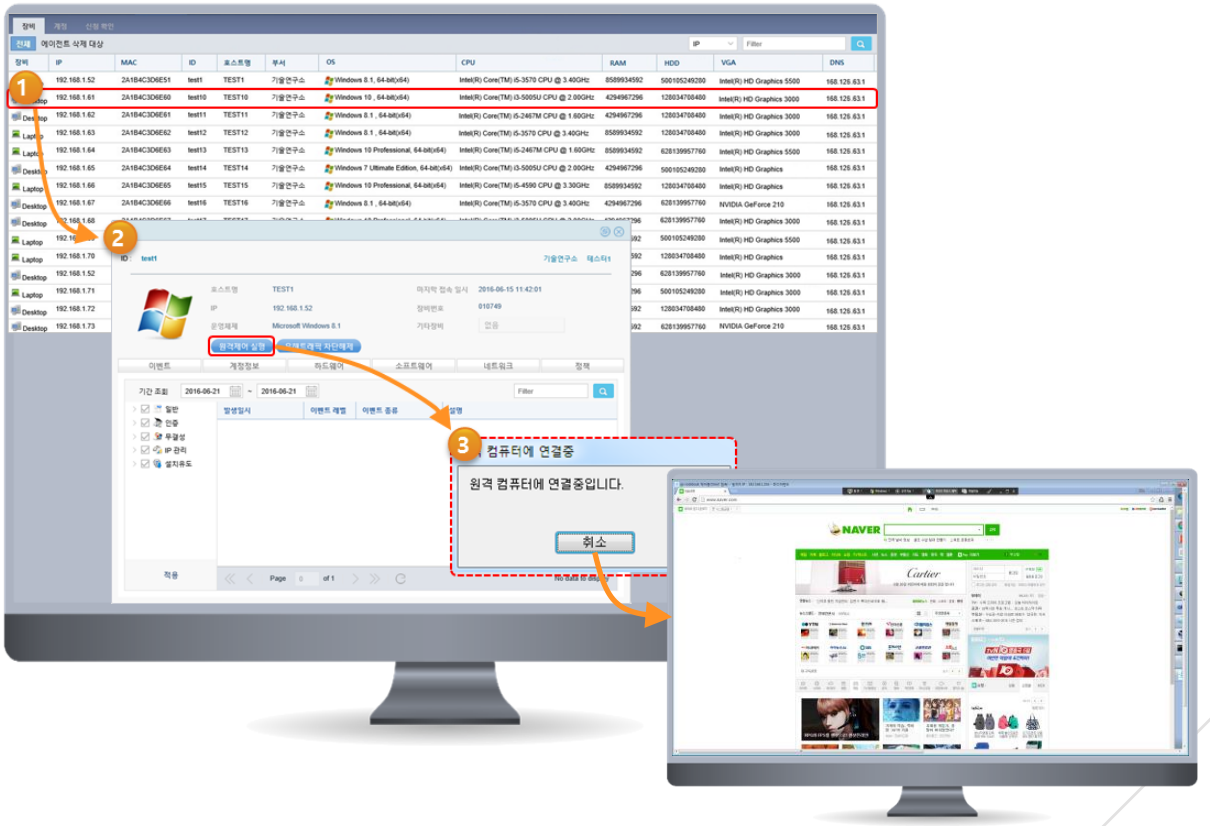
PC 원격 제어

- 장애 발생 PC에 대한 실시간 원격제어
- 동시에 여러 대의 PC 동시 원격 제어
- LAN, WAN 구간에 관계 없이 지원
- 원격제어 속도 향상
- 제어 시 사용자 허락 등 보안 옵션
- 원격제어 로그 기록

부가 서비스

- 1 : 1 파일 전송
- 부서별, 사용자 별 메시지 전송
- 관리자와 사용자간 채팅

관리자 원격 지원



전원관리

출근 전 및 퇴근 후 PC의 사용을 차단 또는 제어하여 업무 외 시간의 이용을 통제

출/퇴근 PC관리

- 정시 출근 및 퇴근을 위한 PC 사용 시간 통제 기능 제공

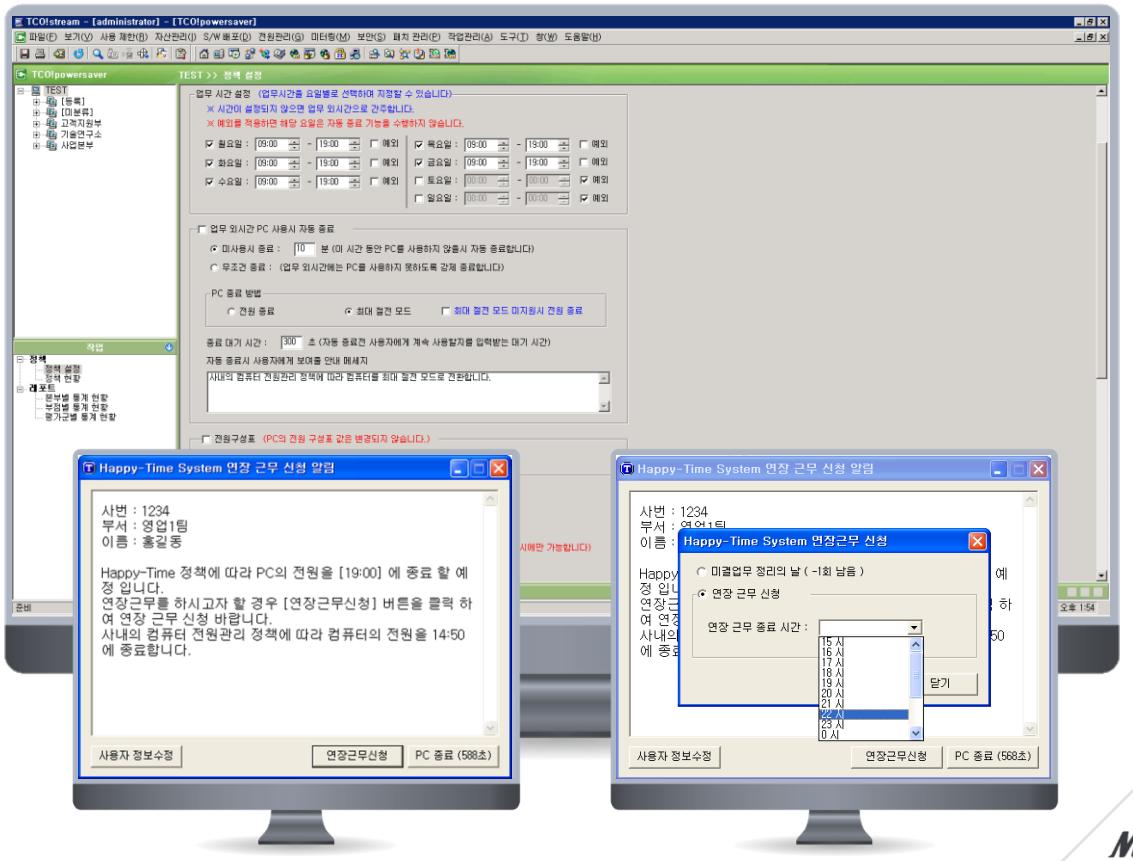
연장 근무 신청

- 인사 시스템과 연동을 통하여 연장 근무 시청자 및 당직 근무자의 PC를 자동으로 제어

PC의 On/Off 관리

- 정해진 시간 외 PC 사용자 이력 관리
  불법 사용 시 강제 PC Off 또는 특정 시간만 허용(기본 10분)

관리자 설정 및 사용자 화면



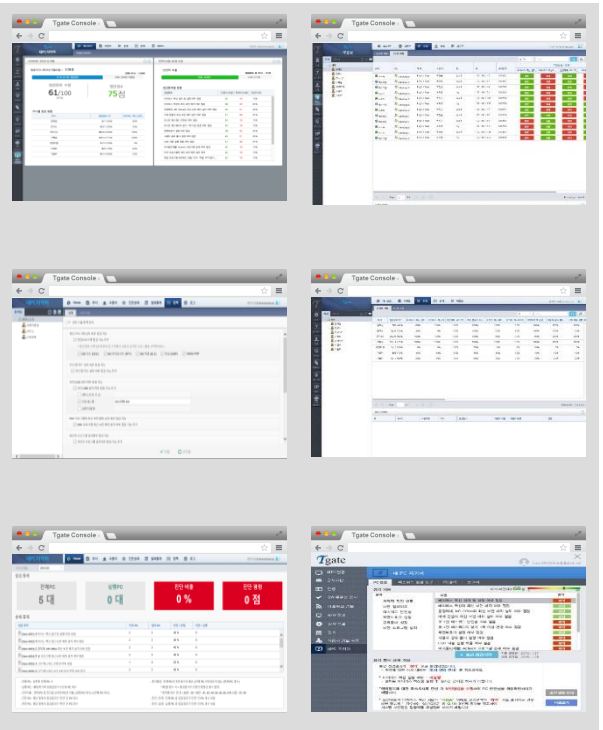
내PC지키미

PC의 취약성을 진단하여 안전한 상태로 개선하며, 조직 전체 PC에 대한 보안 수준 유지

기능 비교

	A사	Tgate 내PC지키미	G사
운영 환경	APC 연계	H/W 일체형 제품	H/W 일체형 제품
최대 사용자	서버당 최대 10,000 node	서버당 최대 **200,000** node (DB 분리 구성)	서버당 최대 100,000 node (DB 분리 구성)
구동 방식	APC 연계 구동 (독립 구동 시, H/W 구축 필요)	독립 구동	독립 구동
점검 항목	국정원 점검 항목 (16개 항목)	국정원 점검 항목(16개 항목) **추가 MS 윈도우 보안 강제화**	국정원 점검 항목 (16개 항목)
취약 항목 처리	취약 항목 One-Click 조치 (통제 기능 無)	취약항목 One-Click 조치 미 조치 시 화면 통제 기능 제공 **네트워크 접근통제 기능 제공**	취약 항목 One-Click 조치 미 조치 시 화면 통제 기능 제공
NAC 연동	타사 NAC 연동으로 제어 가능	Agent 통합 설치 운영 지원	Agent 통합 설치 운영 지원
기술 지원	On/off-line 기술지원	**본사/협력사 기술 지원 제공** **On/off-line** 기술지원	협력사를 통한 간접 기술지원
	LOW	HIGH	MEDIUM

관리자 콘솔





Tgate 특강점

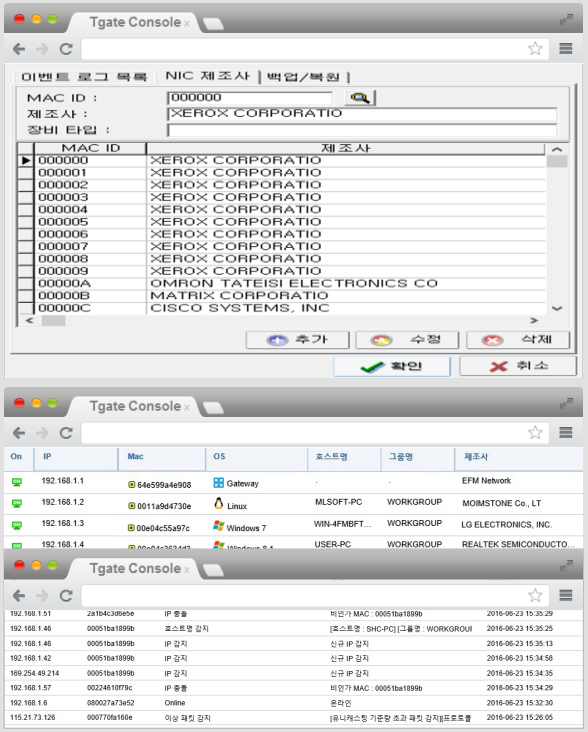
Agentless 기반 통제

네트워크에서 발생되는 모든 신호를 확인하여 등록된 단말 외 완벽한 차단

Agent-less 기능

구분	주요 기능	상세 내용
Agent-less (IP관리)	IP 수집 및 관리	네트워크에 접속된 모든 장비의 **IP, MAC,** 호스트명 등의 자원 정보 수집 다중 **MAC,** 다중 **IP**를 가진 장비 관리 가능 **802.1Q**를 지원하여 **1**대의 장비로 최대 **128**개 **VLAN** 대역을 관리 가능
	IP충돌방지 및 중요 장비 보호	방화벽, **Router, DNS, Main-Host** 등 중요 장비 보호 사내 중요 사용자의 **PC IP** 충돌 원천적 방지 **IP** 대역 내 기준치 이상의 **ARP** 브로드캐스팅 발생 시 통제 **(**임계치 설정**)**
	불법 **IP** 및 **MAC**차단	허가되지 않은 **IP** 및 **MAC** 감지 차단
	DHCP서비스	클라이언트의 **IP** 할당을 지속적인 고정 할당이 가능 미리 **IP**를 예약하여 요청이 오면 예약된 **IP**를 할당이 가능
	Platform DB 제조사 정보	**MAC** 제조사 정보를 주기적으로 업데이트하여 최신의 분류 정보 제공 약 **20,000** 개 이상의 **Platform** 정보 리스트
	이벤트 통계 및 보고서	관리 정책에 대한 **Log** 수집 및 결과 분석 네트워크에서 발생하는 이벤트 기록 및 조회 사용자의 **IP/MAC** 사용 내역을 추적

플랫폼 DB, 실시간 이벤트



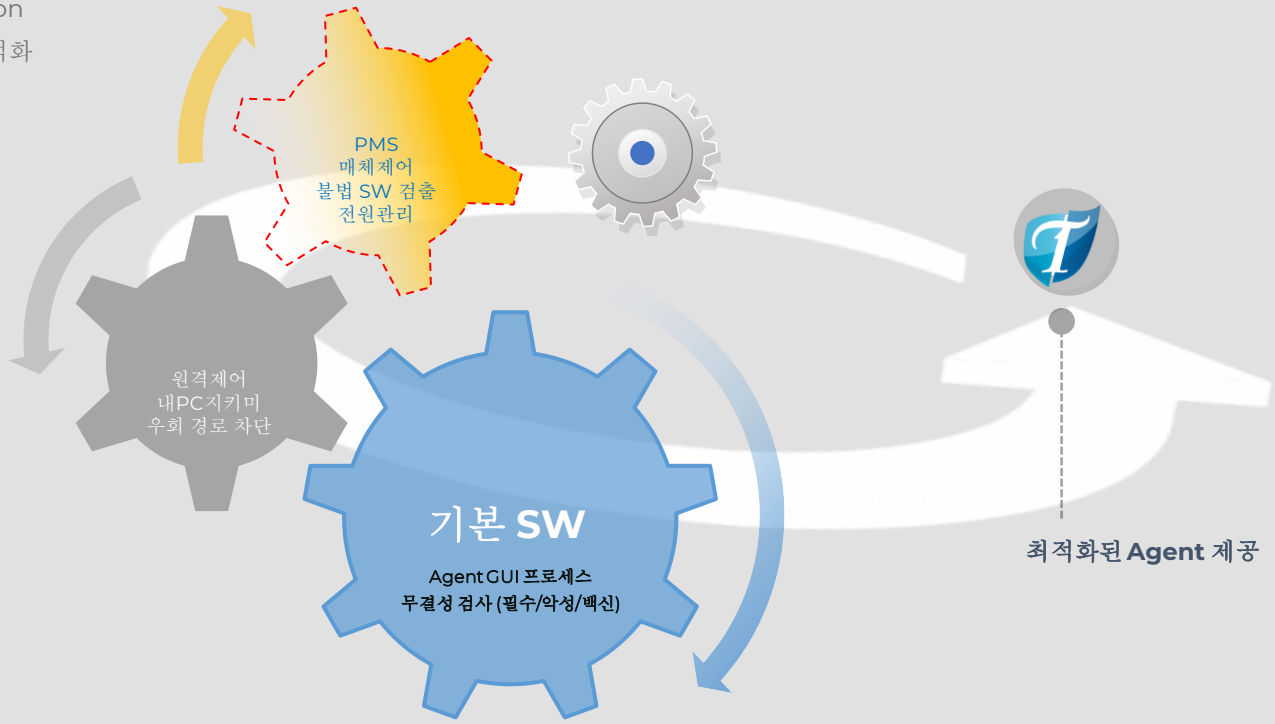
Add-on 동작 추가 기능

Agent 방식 동작 기능을 Add-on 형태로 추가하여 필요한 프로세스만 구동 불필요한 동작 제거

Add-on 형태로 구현

Agent 형태로 동작하는 모든 프로세스는 Add-on 형태로 제공하여 필요한 기능만 동작 리소스 최적화

1. 기본 SW (Agent GUI)
2. PMS
3. 원격제어
4. 매체제어
5. 내PC지키미
6. 불법 SW 검출
7. 우회 경로 차단
8. 전원관리



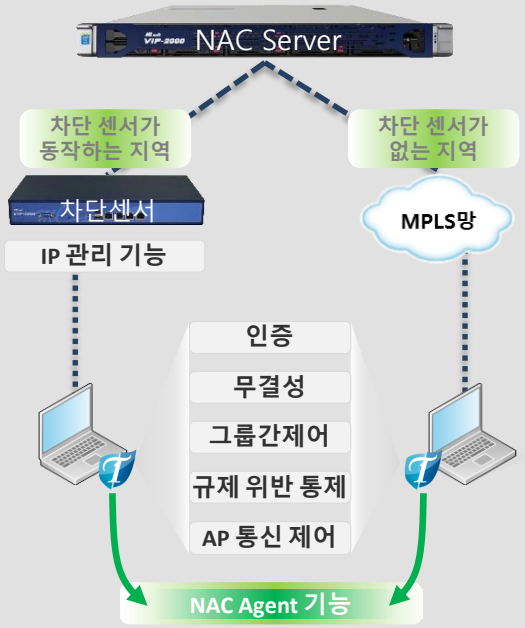
Agent 독립적인 차단 기능

차단 센서가 위치 할 수 없는 지역 및 소규모 사업장에서 장비에 의존없이 NAC 기능 수행

기능

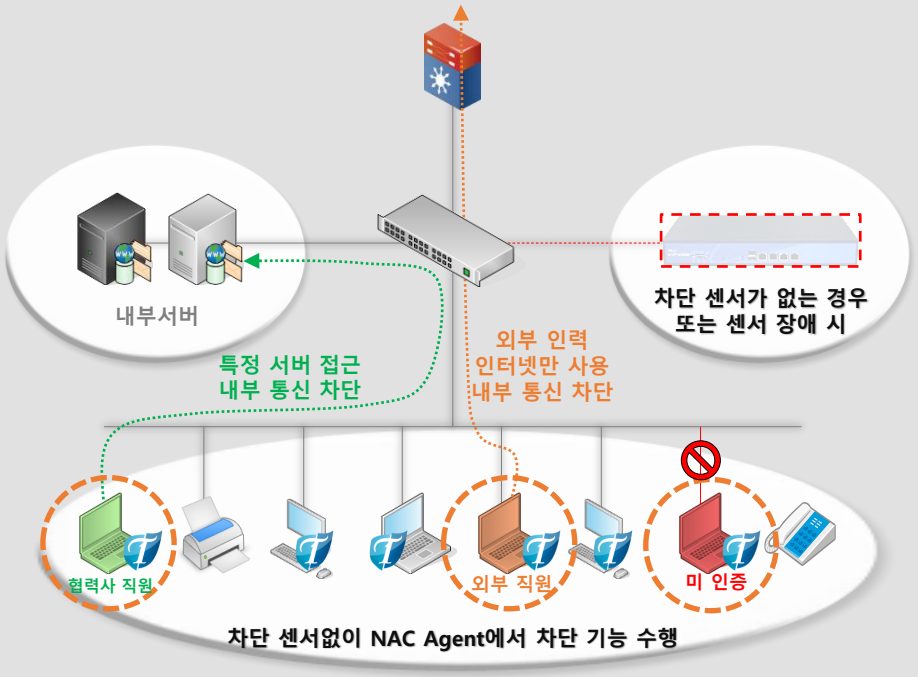
❖ 차단 센서와 NAC Agent의 독립적 수행함으로써 차단 센서의 부하를 줄여 장비 오작동 방지

(장비에서만 차단 할 경우 부하가 집중되 Down 현상 발생)



구성

❖ 차단 센서 없거나 장애 시 NAC Agent에서 통제 기능 유지

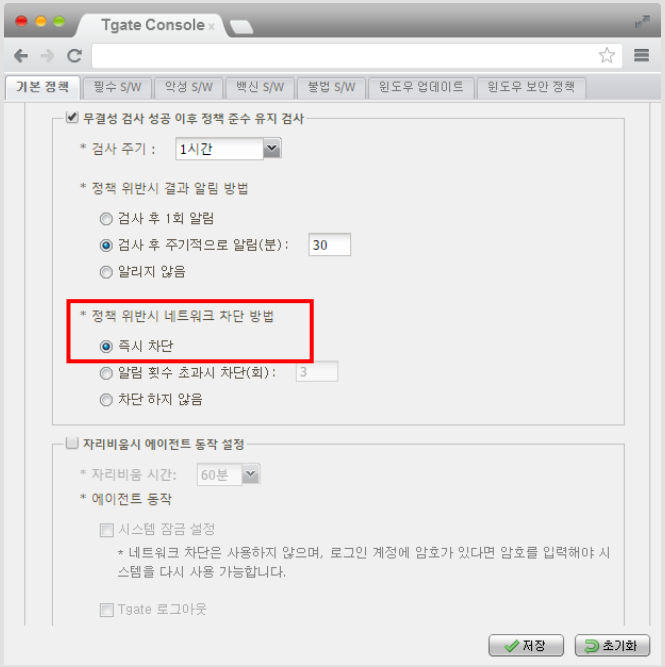


사용자 통제 및 알림 (Real-time)

사용자의 규제 위반 시 Web을 실행하지 않고 실시간으로 사용자 알림 및 설치 유도 진행

정책 설정

- 알림 횟수 초과 시 네트워크 차단
- 차단된 위반 정책의 내용 자동 POPUP



사용자 실시간 알림

- 사용자의 규제 위반 시 Agent를 통한 사용자 알림 기능
- 통제에 대한 사유를 실시간 안내하여, 사용자의 빠른 대처 및 보안의식 고취

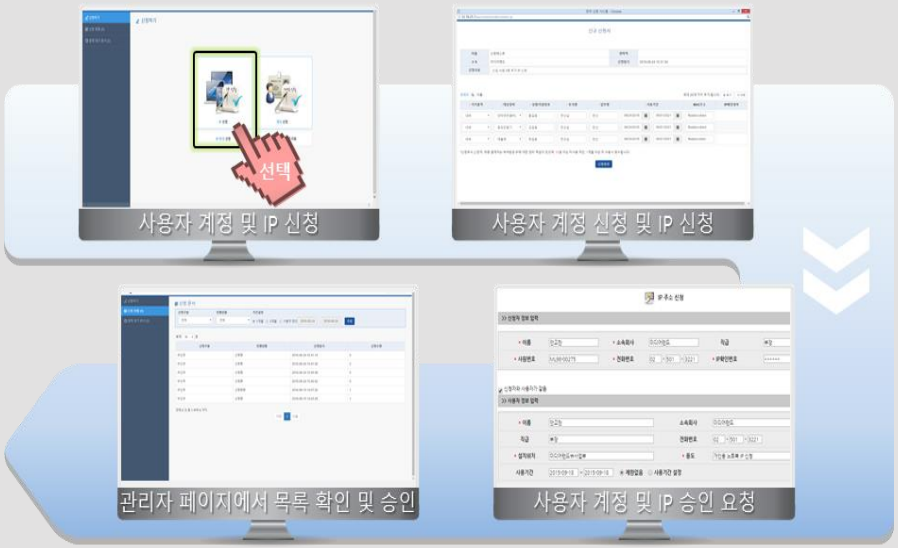


IP 실명제 신청 시스템

사용자 로그인을 통한 본인 확인 정보 및 IP 신청 시스템의 접수로 IP 실명제 구축

IP 및 계정 신청 시스템

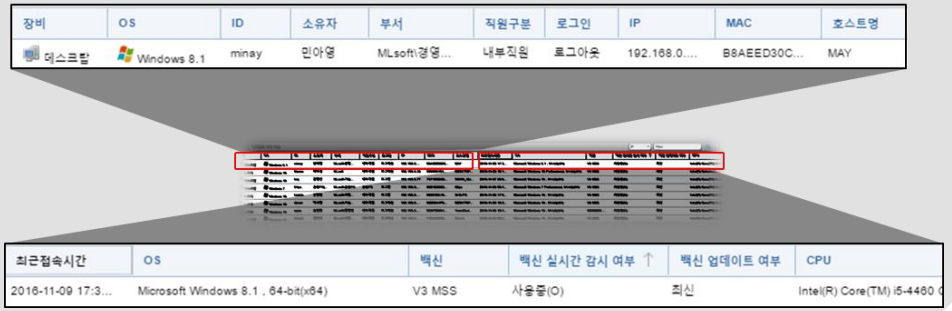
- IP 신청 시스템을 통한 IP 자동 할당
- 외부 직원 및 협력 직원 계정 신청
- IP차단 시에 사용자가 신청하고 승인할 수 있는 절차를 제공



사용자 정보 수집

- IP 신청 시스템을 통한 사용자 정보와 Agent에서 수집된 H/W, S/W 정보로 관리자에게 정확한 정보 제공



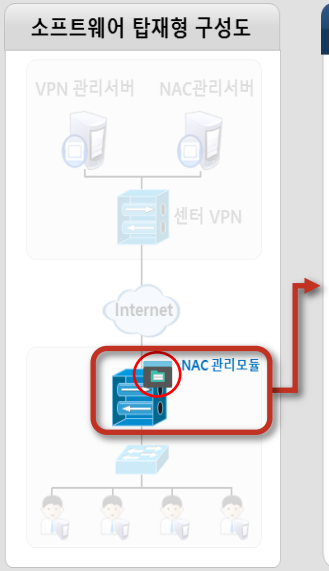


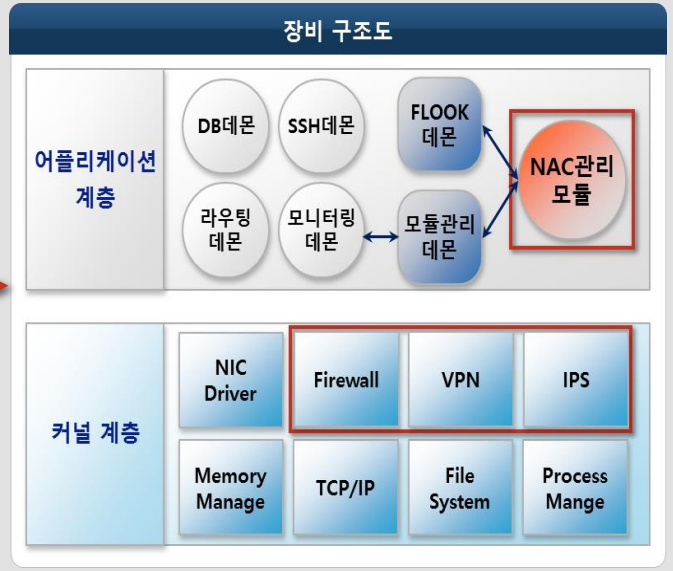
VPN, UTM 탑재형 센서

차단 센서 10,000개 이상 VPN에 탑재형 센서로 구축한 경험을 통한 성능 검증과 안전성 확보 및 비용 절감

VPN/UTM 탑재형 구성 및 동작 구조

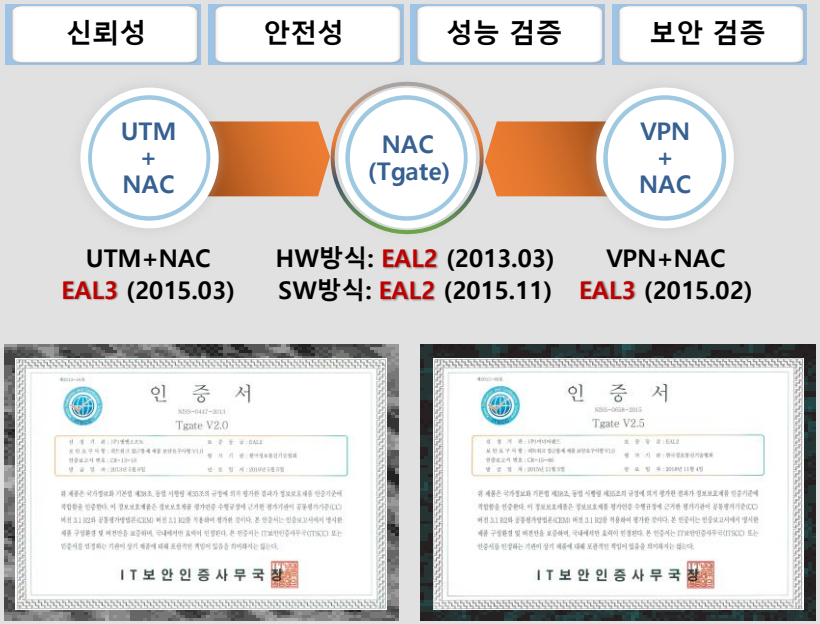
- 기존 VPN, UTM 장비에 SW모듈을 탑재하여 운영
- 어플리케이션/커널 간의 독립적인 운영
- VPN/UTM 장비의 성능저하 방지 데몬 프로세스 동작
- 10,000개 탑재형 장비에서 NAC 모듈로 인한 오동작 제로 퍼센트 유지 중





CC 인증

- H/W 및 S/W 방식에 대한 Tgate CC인증
- UTM, VPN 탑재에 대한 보안장비 업체 CC인증 획득





인증서

인증서

CC인증(EAL2), GS인증(1등급), 특허등록 및 조달청 등록 제품



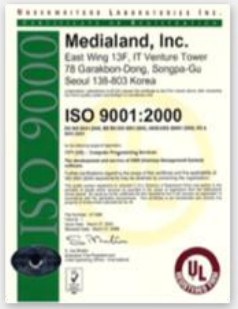
CC 인증



GS 인증서



특허증



ISO 9001



행정업무용 소프트웨어 인증

- 공인된 기관의 인증을 통한 안전성과 신뢰성 보장
- IT보안인증사무국 CC인증 (EAL2)
- Window10 CC인증 획득
- GS인증 (1등급) 획득
- 특허 등록 및 ISO 9001 인증
- 행정업무용 소프트웨어 선정 및 조달청 등록

MLsoft
Pioneer of Endpoint Management



구축사례

유사 구축 실적

공공기관 및 금융권 구축 실적

발주처	사업명	납품일	납품내역	참여형태
농협은행	IP주소 관리 시스템 업그레이드 구축	2020.11 ~ 2021.03	NAC (agent-less)	주사업자
수협중앙회	네트워크 관리 통제 시스템 고도화	2021.10 ~ 2021.12	NAC	주사업자
신한은행	네트워크 접근 제어 고도화 구축	2022.05 ~ 2022.06	NAC	주사업자
IBK기업은행	네트워크 접근 제어 구축	2015.07 ~ 2015.09	NAC	주사업자
ETRI	네트워크 접근 제어 구축	2020.10 ~ 2020.12	NAC	주사업자
금융감독원	네트워크 접근 제어 구축	2017.04 ~ 2017.06	NAC	주사업자
금융보안원	네트워크 접근 제어 구축	2018.02 ~2018.05	NAC	주사업자
한국수력원자력	업무망 NAC 고도화 구축 인터넷망 NAC 구축	2022.04~2022.05	NAC	주사업자
통계청	네트워크 접근 제어 구축	2021.04~2021.05	NAC	주사업자
산림청	네트워크 접근 제어 구축	2022.02~2022.04	NAC	주사업자
해양경비안전본부	네트워크 접근 제어 구축	2019.11~2020.02	NAC	주사업자

공공기관 및 정부기관의 NAC 도입

본 제안 솔루션은 국내 최대의 에너지 발전소인 한국수력원자력의 본점 및 전국 발전소에 약 50,000개의 IP를 성공적으로 구축하였으며, 국가 중앙 통계기관인 통계청에 네트워크 접근통제 솔루션 구축을 통해 IP실명제 및 사용자 인증을 통한 강력한 보안 시스템의 역할을 지속적으로 수행하고 있습니다.

국내 최대 에너지 발전소 "한국수력원자력"

구축개요

- 본점 및 원자력/수력/양수 전국 22개 발전소 50,000 IP 구축
- 중앙 집중 Endpoint 보안 정책 및 네트워크 접근 통제 체계 운영

요구사항

- IP기반으로 한 네트워크접근통제
- 계정 시스템 및 타 솔루션과 연동을 통해 중추 시스템 역할
- 본점 및 원자력/양수/수력 전국 발전소 30,000 node Endpoint 통제
- 추가 해외 지점 NAC 구축 (UAE, 타지키스탄 등)

IP/MAC 자원의 중앙 통합 관리 | **사내 보안 정책에 의한 관리강화** | **네트워크 접근 전 차단**

국가 중앙 통계기관 "통계청"

구축개요

- 본청 및 지방청 10,000 IP 구축
- 내/외부 사용자 통제 및 그룹간 제어, 강력한 Agent 기반 방식의 규제준수 적용

요구사항

- 전국 영업점 네트워크접근통제 솔루션 구축
- 인터넷 접속 구간
- 본접 및 영업점 점 15,000개 IP (영업점 680개)
- 망분리 및 PMS 등 연계
- Agent 방식의 네트워크접근통제

신규 인터넷망 보안 시스템 적용 | **전국 영업점 NAC 센서 구축** | **Agent 방식의 인증**

제1금융권의 NAC 도입

본 제안 솔루션은 국내 최다 지점을 보유한 NH농협은행에 약 30만개의 IP를 성공적으로 구축하였으며, 금융을 감독하는 기관의 IP실명제시스템을 적용하여 네트워크접근 통제 체계 운영을 성공적으로 수행하고 있습니다.

국내 최다 지점 IP관리 도입 "NH농협은행"

구축개요

- 중앙회 / 본사 및 약 13,000여 개 지점 구축
- 기존 IP관리 대체 구축기술력과 IP기반 네트워크 접근통제 구축

요구사항

- 국내 최다지점 IP관리 시스템 구축
- 농협은행 및 중앙회 / 본사 및 약 13,000여 개 지점 구축
- 관리 IP : 총 **300,000개**
  - PC : 100,000개
  - 기타 : 100,000개 이상 (Network 장비 및 ATM 등)
- BMT, 기술협상을 통한 **단독 선정**
- AD연동 및 웹을 통한 사용자 인증으로 IP실명제 구축
- 보안포털 시스템과 연동을 통한 결재 시스템 적용

AD 연동 | **연동을 통한 결재시스템 적용** | **사용자 인증**

금융감독기관 "금융감독원"

구축개요

- 논리적 망분리 구축시 비용절감 및 네트워크접근통제 체계 강화
- 사용자 인증을 위한 AD연동을 통해 설계사 인증 IP실명제 구현

요구사항

- 금융기관 최상위 컴플라이언스 수행
- 계정 시스템 및 타 솔루션과 연동을 통해 중추 시스템 역할
- 원내 시스템 연동
- 감독기관 본원등 12개소
- 총 65개 대역 (IP 4,000개)



IP 실명제 구현 | **IP주소 신청시스템 구축** | **사용자 인증시스템**

MLsoft
Pioneer of Endpoint Management

금융 및 정부기관의 NAC 도입

본 제안 솔루션은 국내1위은행 신한은행 본점 및 지점에 약 70,000개의 IP를 성공적으로 구축하였으며, 타사 IP관리시스템을 대체하는 뛰어난 성능으로 구축 후 3년동안 사내 보안정책을 통한 네트워크접근 통제 체계 운영을 성공적으로 수행하고 있습니다.

국내 1위 은행 NAC 도입 "신한은행"

구축개요

- 본점/지점 1,000여개 전국 지점의 약 70,000개의 IP 구축
- 3년 동안 사내 보안 정책 및 네트워크접근통제 체계운영

요구사항

- IP기반으로 한 네트워크접근통제
- 계정 시스템 및 타 솔루션과 연동을 통해 중추 시스템 역할
- 기존 IP관리 **시스템 최단기간 교체 구축** (영업점 : 2주)
- 본점/지점 70,000개 IP (약 1,000개 지점)
- 추가 해외 지점 IP 관리

IP/MAC 자원의 중앙 통합 관리 | **사내 보안 정책에 의한 관리 강화** | **네트워크 접근 전 차단**

NAC를 통한 실명제 "ETRI"

구축개요

- 연구동 및 인터넷망 보안 무결성을 위한 NAC 시스템 구축
- 불법 SW 및 기타 규제 위반 단말 통제 체계 운영

요구사항

- ETRI 본원 및 지역 연구동의 IP 실명제
- 사용자의 불법 SW 사용 현황 파악 및 통제
- IP/MAC/사용자의 정보 일치 및 단말 위치 파악
- 기 사용중인 3rd Party 시스템 로그인 연동 (SSO)
- Agent 방식의 네트워크접근통제

본원 및 지역 연구동 IP 실명제 | **불법 SW 및 규제 미 준수 단말 통제** | **Agent 방식의 인증**

MLsoft
Pioneer of Endpoint Management



주요 고객사

주요 고객사

공공

통계청 | 산림청 | 관세청
행정자치부 | 국토교통부 | 보건복지부
교육부 | 국가기록원 | 국민안전처
외교부 Ministry of Foreign Affairs | 군사안보지원사령부 Defense Security Support Command | 국군지휘통신사령부 DEFENSE COMMUNICATION COMMAND
한국수력원자력 | 경찰청 KOREAN NATIONAL POLICE AGENCY | 해양경찰청 KOREA COAST GUARD
K water 한국수자원공사 Korea Water Resources Corporation | 한국가스공사 | 한국지역난방공사

금융

금융감독원 | 금융보안원 FINANCIAL SECURITY INSTITUTE | KDIC 예금보험공사 Korea Deposit Insurance Corporation
Sh 수협은행 | 신한은행 | 참! 좋은 은행 IBK기업은행
KYOBO 교보증권 | lifeplanet 교보라이프플래닛생명 | IBK 기업은행 금융그룹 IBK 연금보험
광주은행 | 한화투자증권 | SB 저축은행중앙회
하나생명 | 하나캐피탈 | 부국증권
롯데손해보험 | NH농협생명 | NH저축은행

기업

대한항공 | 한진해운 | JEJUair
SAMSUNG 삼성SDS | 현대상선 HYUNDAI MERCHANT MARINE | HYUNDAI ELEVATOR CO., LTD.
쌍용자동차 | BMW Handok Motors | HANKOOK driving emotion
hankookilbo | Dongwha | SEAH
홈&쇼핑 | netmarble | com2us 컴투스
(주)롯데주류 | 롯데백화점 | 롯데리아

의료

국립암센터 NATIONAL CANCER CENTER | 서울특별시 서울의료원 Seoul Medical Center | 인천광역시의료원 INCHEON MEDICAL CENTER
SAMSUNG 강북삼성병원 | 연세대학교 의료원 YONSEI UNIVERSITY HEALTH SYSTEM | 강남세브란스병원 GANGNAM SEVERANCE HOSPITAL
용인세브란스병원 YONGIN SEVERANCE HOSPITAL | 인하대병원 www.inha.com | 순천향대학교병원
NCMH 국립정신건강센터 | KMI 재단법인 한국의학연구소 KOREA MEDICAL INSTITUTE | NRC 국립재활원 National Rehabilitation Center
국립소록도병원 Sorokdo National Hospital | BN 국립부곡병원 BUGOK NATIONAL HOSPITAL | 제주대학교병원 JEJU NATIONAL UNIVERSITY HOSPITAL
국립나주병원 NAJU NATIONAL HOSPITAL | 국립공주병원 Gongju National Hospital | 국립목포병원 Mokpo National Tuberculosis Hospital

THANK YOU
FOR WATCHING

㈜엠엘소프트 안교찬 이사

E-mail. kyochan7@mlsoft.com

Tel. 010-4390-5200

www.mlsoft.com

서울시 영등포구 양평로 21가길 19, 우림라이온스밸리 B동 7층