통합 보안 플랫폼 기업, 지니언스

# Cloud Genian NAC

Genians

# Table of Contents

# 01.

# 배경 및 필요성

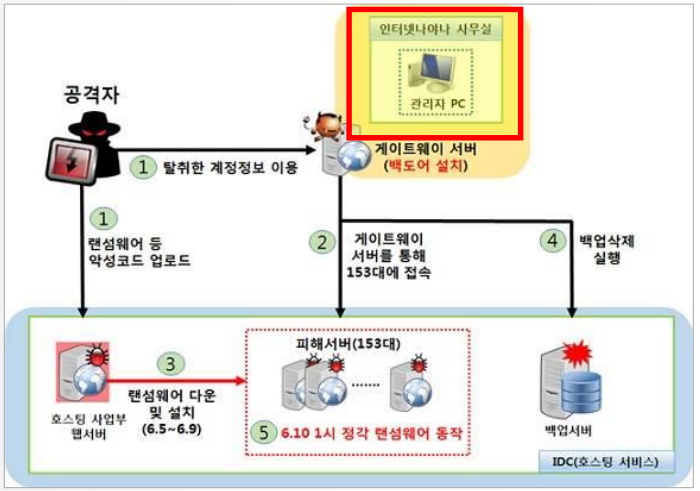
# 지속적인 기술유출/보안사고

## “전통적인 방법의 기술 유출과 지능적인 해킹”

**대표적 공격 종류 3가지**

1. 기술 유출 및 외부 공격 위험 : 외부에서 접근 가능한 장치들이 회사 내부에 접근 할 수 있는 환경
2. 장치 인증 및 소셜 엔지니어링 : 인증되지 않는 장치 및 사용자가 내부에 접근 / 청탁을 통한 내부 관계자 접근
3. 악성 소프트웨어 감염 : 보안패치가 적용되지 않은 장치의 사용으로 취약점에 노출된 장치인한 정보 유출 가능성 높음

### 외부 위협과 내부 관계자 및 내부 보안관리 부재로 인한 피해 증가

# ISMS 기준 대비 NAC 도입 타당성

## ISMS-P 인증기준 안내서 (2023.10.31 기준)

### ISMS-P 법적근거


- 정보통신망 이용촉진 및 정보보호에 관한 법률 제47조
- 정보통신망 이용촉진 및 정보보호에 관한 법률 시행령 제47조~제54조
- 정보통신망 이용촉진 및 정보보호에 관한 법률 시행규칙 제3조
- 개인정보보호법 제32조의2
- 개인정보보호법 시행령 제34조의2~제34조의8
- 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시

**외부자 보안** 보호대책 요구사항 2.10.6 (업무용 단말 기기 보안)

보안시스템 접근통제 정책(사용자 인증, 관리자 단말 IP / MAC

**정보자산 분류** 관리체계 수립 및 운영 1.2.1 (정보자산 식별 세부 설명)

정보자산의 분류기준을 수립, 자산 식별하여 목록 관리

**물리적 보안** 보호대책 요구사항 2.5 (인증 및 권한 관리)

정보시스템 및 개인정보 시스템 접근 시 보호대책 마련

**접근통제** 보호대책 요구사항 2.6 (접근통제)

업무상 중요 정보가 비인가자에게 유출되지않도록 보호대책 마련

**무선통신통제** 보호대책 요구사항 2.6.5 (무선 네트워크 접근 통제)

무선 네트워크 사용하는 경우 사용자 인증 및 통제 보호대책 마련

**개인정보보호위원회 개인정보의 안정성 확보 조치 기준**

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol) 주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP (Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응

**방송통신위원회 정보보호 관리지침**

② 시스템관리자는 각종 서버·PC 정보통신장비 등 정보시스템이 비인가자에게 허용되지 않도록 보안기능을 설정하여야 한다.
③ 시스템관리자는 보안도구를 이용하여 정보시스템의 보안취약점을 진단하여야 하며, 시스템 접속시 다음 각 호의 사항이 자동 저장되도록 하여야 한다.
1. 서버 접속일시, 접속자 및 접속방법 등 정보통신망 접근기록(1차)
2. 전산자료 열람·출력 등에 대한 사용자, 일시, 자료제목 등 접근기록(2차)
④ 시스템관리자는 다음 각 호와 같이 자동 수록된 접근자료(Log Data)를 관리하여야 한다.
1. 접근자료는 접속의 성공여부와 상관없이 기록 유지

**의료기관 개인정보보호 가이드 라인**

| | |
|---|---|
| 기술적 조치 | ▹ 접근 권한의 제한·관리<br>▹ 접근통제 시스템 설치 및 운영<br>▹ 개인정보 암호화<br>* 주민번호를 보관 시에는 반드시 암호화하여야 함<br>▹ 접속기록의 보관 및 위·변조 방지<br>▹ 보안 프로그램의 설치·운영<br>▹ 관리용 단말기의 안전조치 |

# ISMS 인증기준항목별 NAC 대응사항

| 영역 | 분야 | 적용 여부 | | NAC 활용/대응 항목 |
|---|---|---|---|---|
| | | ISMS | ISMS-P | |
| 1. 관리체계 수립 및 운영 (16개) | 1.1. 관리체계 기반 마련 | ○ | ○ | |
| | 1.2. 위험 관리 | ○ | ○ | 1.2.1 정보자산 식별 |
| | 1.3. 관리체계 운영 | ○ | ○ | |
| | 1.4. 관리체계 점검 및 개선 | ○ | ○ | |
| 2. 보호대책 요구사항 (64개) | 2.1. 정책, 조직, 자산 관리 | ○ | ○ | |
| | 2.2. 인적 보안 | ○ | ○ | 2.2.3 보안서약 |
| | 2.3. 외부자 보안 | ○ | ○ | 2.3.2 외부자 계약 시 보안 |
| | 2.4. 물리 보안 | ○ | ○ | 2.4.7 업무환경 보안 |
| | 2.5. 인증 및 권한관리 | ○ | ○ | |
| | 2.6. 접근통제 | ○ | ○ | 2.6.1 네트워크 접근<br>2.6.5 무선 네트워크 접근<br>2.6.6 원격접근 통제*<br>2.6.7 인터넷 접속 통제* |
| | 2.7. 암호화 적용 | ○ | ○ | |
| | 2.8. 정보시스템 도입 및 개발 보안 | ○ | ○ | |
| | 2.9. 시스템 및 서비스 운영관리 | ○ | ○ | |
| | 2.10. 시스템 및 서비스 보안관리 | ○ | ○ | 2.10.6 업무용 단말기기 보안<br>2.10.7. 보조저장매체 관리 |
| | 2.11. 사고 예방 및 대응 | ○ | ○ | |
| | 2.12. 재해복구 | ○ | ○ | |
| 3. 개인정보 처리 단계별 요구사항 (22개) | 3.1. 개인정보 수집 시 보호조치 | - | ○ | |
| | 3.2. 개인정보 보유 및 이용 시 보호조치 | - | ○ | |
| | 3.3. 개인정보 제공 시 보호조치 | - | ○ | |
| | 3.4. 개인정보 파기 시 보호조치 | - | ○ | |
| | 3.5. 정보주체 권리보호 | - | ○ | |

※ 2023년 11월 23일 기준

**1.2.1 정보자산 식별**

- 조직의 업무특성에 따라 정보자산 분류 기준 수립 및 모든 자산 식별·분류

**2.2.3 보안 서약 / 2.3.2 외부자 계약시 보안**

- 정보자산 취급 및 접근권한이 부여된 임직원에 대해 법규와 비밀 유지의 고지 및 정보보호 서약
- 중요정보 및 개인정보 처리 관련 서비스를 위탁 선정하는 경우 정보보호 개인정보보호 요구사항 식별 및 관련 내용을 계약서에 명시하고 절차 마련

**2.4.7 업무환경 보안**

- 문서고, 공용PC, 복합기 파일서버 등 공용사용 시설 사무기기에 대한 보호, 업무환경을 통해 비인가자에게 노출 유출 되지않게 클린데스크 정기점검 대책 수립 및 이행

**2.6.1 네트워크 접근 / 2.6.5 무선 네트워크 접근**

- 네트워크에 대한 비인가 접근을 통제하기 위해 IP관리, 단말인증 관리 절차 수립·이행

* 2.6.6~7 항목은 ZTNA 제품에서 지원

**2.10.6 업무용 단말기기 보안 / 2.10.7 보조저장매체 관리**

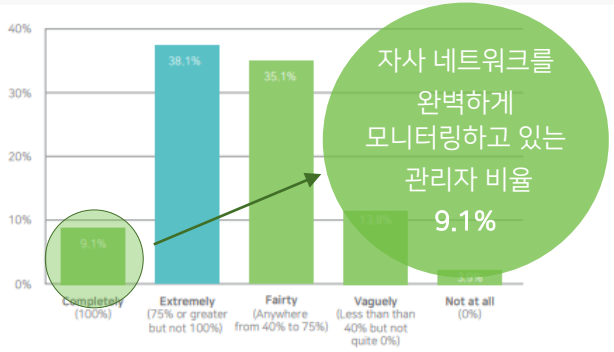
- PC,모바일,가상PC,태블릿 등 사용되는 단말기 기기인증, 승인, 접근범위 설정, 기기보안설정 통제 정책 마련 및 수립·이행
- 외장하드, USB메모리, CD등 보조 저장매체 취급(사용/미사용 제어), 보관 폐기, 재사용에 대한 정책 절차 수립 및 이행

[ISMS 인증기준과 NAC 활용 분야 대비]

# Genian NAC의 가시성

## 네트워크, 사용자, 단말 상태에 대한 가시성 확보 및 상태에 따른 통제 필요

### 네트워크 가시성




<출처 : SANS BYOD Security Survey>

네트워크 단말의 수량 및 다양성 증가↑

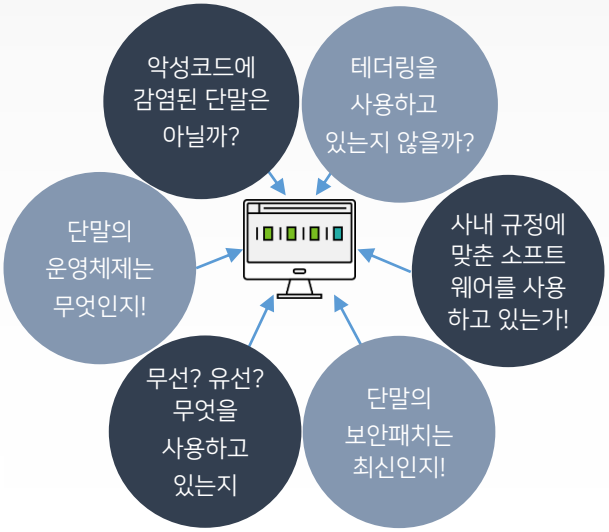
### 사용자 가시성

다양한 인사DB 연동(조직도 연동)


| IP주소 | | MAC주소 | 인증사용자 | 플랫폼 |
|---|---|---|---|---|
| 172.29.114.94 | V6 | 2C:F0:5D:23:31:84 | user1 | Microsoft Windows 10 Professional x64 |
| 172.29.25.144 | V6 | A4:5E:60:F1:D3:4B | user2 | Apple Device |
| 172.29.59.194 | V6 | 18:C0:4D:DE:7D:50 | user3 | Microsoft Windows |

사용자/ 부서별 정책 관리

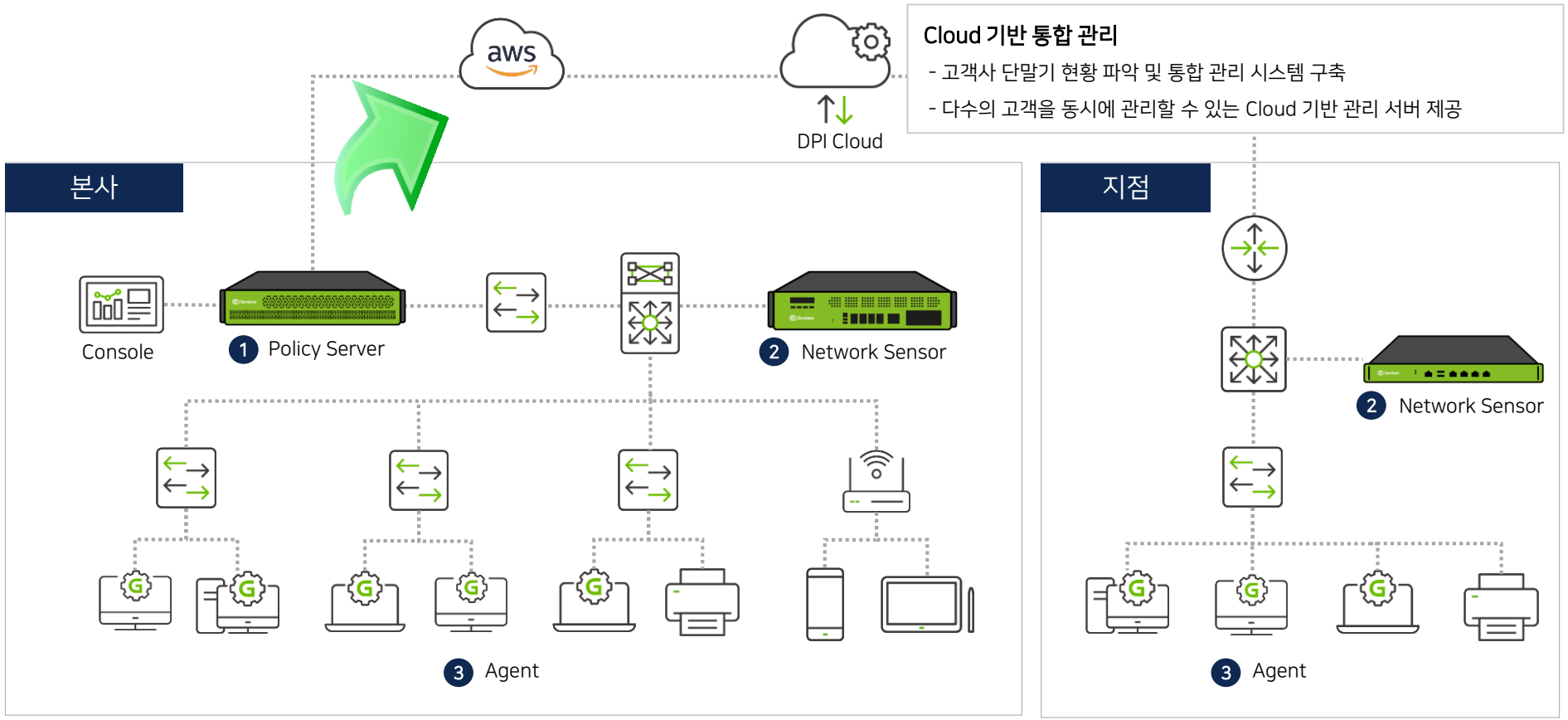
### 단말 가시성



02.

# Genian NAC 제품소개

# NAC 구성




**1 Policy Server & Console (정책서버 & 콘솔)**

- 유무선 네트워크를 통합 관리하고 내부 보안을 강화할 수 있도록 지원

**2 Network Sensor (차단센서)**

- 유무선 단말에 대한 정보를 수집하고 강력한 통제 수행
- 포트 별 802.1Q 설정을 통한 효율적인 운영 지원

**3 Agent (에이전트)**

- PC 등 에이전트 설치 단말에 대한 자산 관리 및 장치사용 통제
- 에이전트 설치에 따른 비용 부담 없음(필요에 따라 선택적 사용)

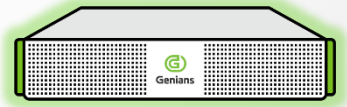
**4 Cloud NAC?**

- 단말 관리 및 제어 플랫폼을 Cloud 기반으로 제공
- 단말 관리 사업을 위해 필요한 다수의 솔루션을 하나의 솔루션으로 대체 가능
- 단일 관리 콘솔 기반으로 각 기능의 유기적 통합 관리 가능

# 제품 특징 비교

## On-premise NAC VS Cloud NAC

### On-premise 방식

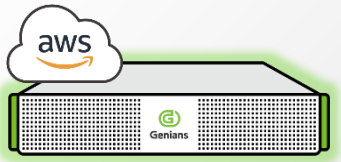



제품형 설치

- CC인증서 획득
- Product 제품 / 정책서버 및 센서장비 설치
- 초기 구매 비용 높음
- 정책 서버 관리 및 서비스 대응 점검 방문 必
- 제품 펌웨어 업데이트 수동 관리
  - 업데이트서버 정책 허용 시 자동업데이트

VS

### Cloud NAC 방식




Cloud Hybrid 설치

- CSAP 인증서 획득
- 정책 서버는 Cloud에서 운영 (SLA 99.95% 보장)
- 서비스 SLA 보상 기준
  - 99.0% 이상 ~ 99.5% 미만 -> 월 요금 10%
  - 95.0% 이상 ~ 99.0% 미만 -> 월 요금 20%
  - 95% 미만 -> 월 요금 30%
- 초기 구매 비용 낮음
- 가장 최신의 펌웨어 자동 업데이트 관리
  - 신규 기능 적용, 최신 보안 업데이트 제공

# 가시성 (1/3)

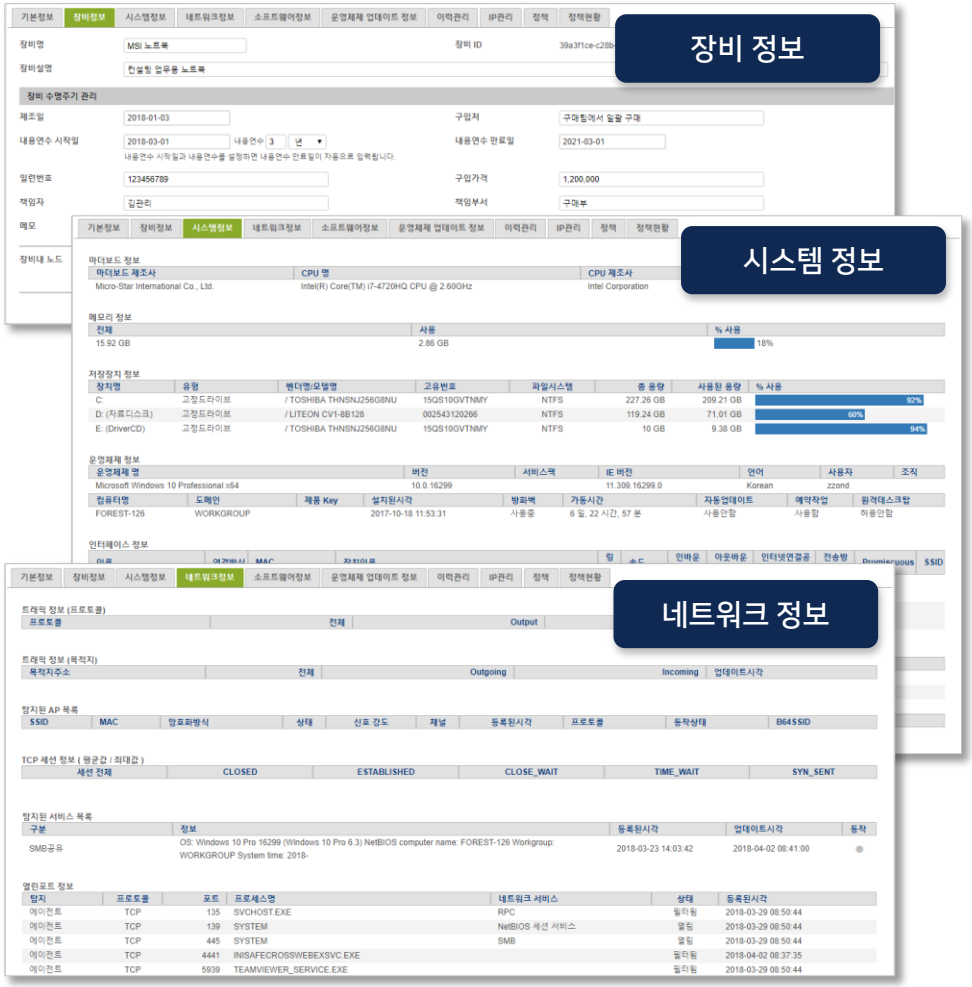
## 네트워크 내의 모든 단말기 정보 수집 및 분류, IP 실명 확인

| 장치구분 | 동작 상태 | 인증정보 | 인증시간 | IP/MAC | | OS/모델 상세 정보 | 적용받는 제어정책 | 관리 센서 | 장비 호스트명 | 일주일간 동작 차트 | 장비명/센서명 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| NT AG SS | 동작 | 인증사용자 | 최근 사용자인증 | IP주소 | MAC주소 | 플랫폼 | 제어정책 | 센서명 | 호스트명(이름) | 동작상태차트 | 장비명 / 센서명 |
| | | 오 | 2022-05-09 09:08:56 | 172.29.20.7 V6 | E0:D5:5E:86:9A:0C | Microsoft Windows 10 Professional x64 | 기본정책 | S-172.29.20.4 | DESKTOP-FMFO9D3 | | S-172.29.20.4 / eth1.20 |
| | | 최 | 2022-02-09 08:26:09 | 172.29.30.207 | 88:36:6C:F5:55:58 | Microsoft Windows 11 Home x64 | 기본정책 | S-172.29.30.4 | 문규 | | S-172.29.30.4 / eth1.30 |
| | | 최 | 2022-02-15 13:29:40 | 172.29.25.76 | B4:B6:76:AB:2E:E4 | Microsoft Windows 10 Professional x64 | 예외허용(EDR개발실) | S-172.29.25.4 | CHOISEOYUN | | S-172.29.25.4 / eth0.25 |
| | | 신 | 2022-02-09 08:32:49 | 172.29.30.142 V6 | 34:29:8F:73:69:32 | Microsoft Windows 11 Home x64 | 디펜더 미동작 차단 | S-172.29.30.4 | 신학선-SHINHS | | S-172.29.30.4 / eth1.30 |
| | | 김 | 2022-02-24 08:34:48 | 172.29.20.18 | 00:E0:4C:62:7A:80 | Microsoft Windows 11 Home x64 | 기본정책 | S-172.29.20.4 | DESKTOP-8A03PN8 | | S-172.29.20.4 / eth1.20 |
| | | 신 | 2022-04-11 13:05:52 | 172.29.25.167 | F4:46:37:8C:16:26 | Microsoft Windows 11 Home x64 | 디펜더 미동작 차단 | S-172.29.25.4 | 신학선-SHINHS | | S-172.29.25.4 / eth0.25 |
| | | 윤 | 2022-02-23 08:25:05 | 172.29.20.129 | 88:36:6C:F8:5F:0D | Microsoft Windows 10 Home x64 | 기본정책 | S-172.29.20.4 | DESKTOP-6G957J9 | | S-172.29.20.4 / eth1.20 |
| | | 유 | 2022-02-15 14:37:07 | 172.29.25.187 | 00:C2:C6:B7:39:D2 | Microsoft Windows 10 Home x64 | GPI 미설치 차단 | S-172.29.25.4 | DESKTOP-4BRJ5H3 | | S-172.29.25.4 / eth0.25 |
| | | 강 | 2022-02-21 08:28:32 | 172.29.20.191 | 00:0A:CD:31:10:90 | Microsoft Windows 10 Home x64 | 예외허용 | S-172.29.20.4 | DESKTOP-HFQGA7S | | S-172.29.20.4 / eth1.20 |
| | | 권 | 2022-03-14 09:33:34 | 172.29.25.102 | 80:32:53:7A:3B:F9 | Microsoft Windows 11 Professional x64 | 기본정책 | S-172.29.25.4 | DESKTOP-QNUAL93 | | S-172.29.25.4 / eth0.25 |
| | | 이 | 2021-10-28 15:12:57 | 172.29.59.33 V6 | 00:0C:29:33:06:27 | Microsoft Windows 7 Professional x64 | 예외허용(EDR개발실) | S-172.29.59.4 | MSLEE-PC | | S-172.29.59.4 / eth0.59 |
| | | 박 | 2022-04-29 11:59:48 | 172.29.25.33 | CC:15:31:F9:29:14 | Microsoft Windows 10 Professional x64 | 기본정책 | S-172.29.25.4 | DESKTOP-QAQ6T18 | | S-172.29.25.4 / eth0.25 |
| | | 안 | 2022-02-16 09:04:49 | 172.29.20.123 V6 | 6C:5A:B0:6C:22:36 | Microsoft Windows 10 Home x64 | 기본정책 | S-172.29.20.4 | Goodrichgil | | S-172.29.20.4 / eth1.20 |
| | | 권 | 2022-02-09 08:08:01 | 172.29.30.129 | 00:E0:4C:62:9E:CC | Microsoft Windows 11 Professional x64 | 기본정책 | S-172.29.30.4 | DESKTOP-QNUAL93 | | S-172.29.30.4 / eth1.30 |
| | | 이 | 2021-10-05 17:27:00 | 172.29.59.32 V6 | 00:0C:29:39:5A:E1 | Microsoft Windows 7 Professional x64 | 예외허용(EDR개발실) | S-172.29.59.4 | MSLEE-PC | | S-172.29.59.4 / eth0.59 |
| | | 이 | 2022-02-24 10:19:37 | 172.29.25.166 | A0:78:17:69:B1:B1 | Apple macOS Monterey | 기본정책 | S-172.29.25.4 | leejsui-MacBookPro.local | | S-172.29.25.4 / eth0.25 |

| GUI Column | Column Description | Column Sample Value |
|---|---|---|
| 인증사용자 | 해당 장비를 사용 중인 인증 사용자 이름 | 오승환 |
| 최근 사용자인증 | 최근 사용자인증을 한 시각 | 2022-05-09 09:08:56 |
| IP주소/MAC주소 | 해당 단말이 사용 중인 IP와 MAC 주소 | 172.29.20.7 / E0:D5:5E:86:9A:0C |
| 플랫폼 | 해당 단말의 플랫폼 | Microsoft Windows 10 Professional x64 |
| 제어정책 | 해당 단말이 적용 받는 네트워크 정책 | 기본정책 |
| 호스트명 | 해당 단말의 호스트명 | DESKTOP-FMFO9D3 |

# 가시성 (2/3)

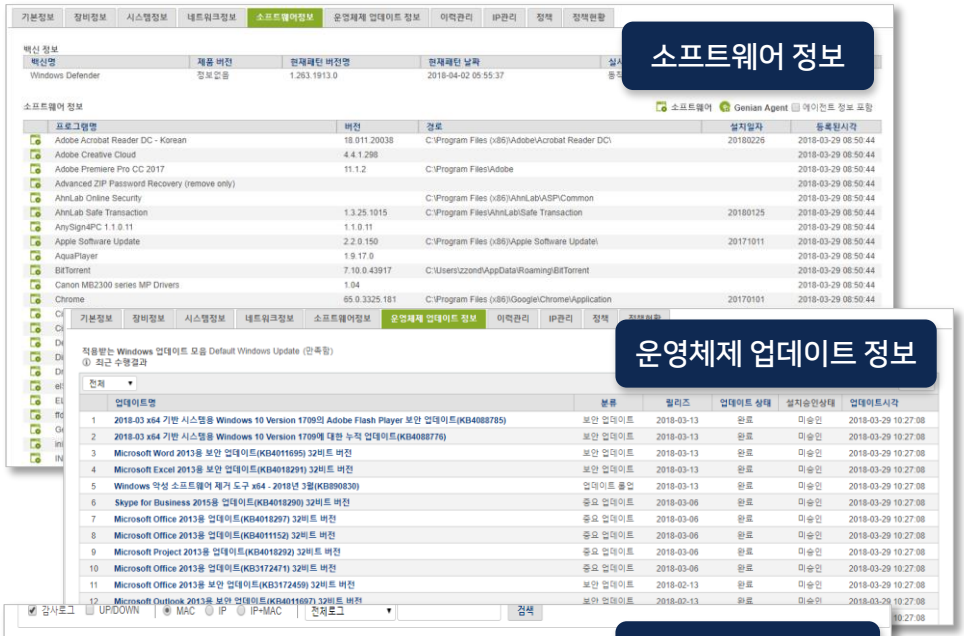
## PC 내의 다양한 정보 제공





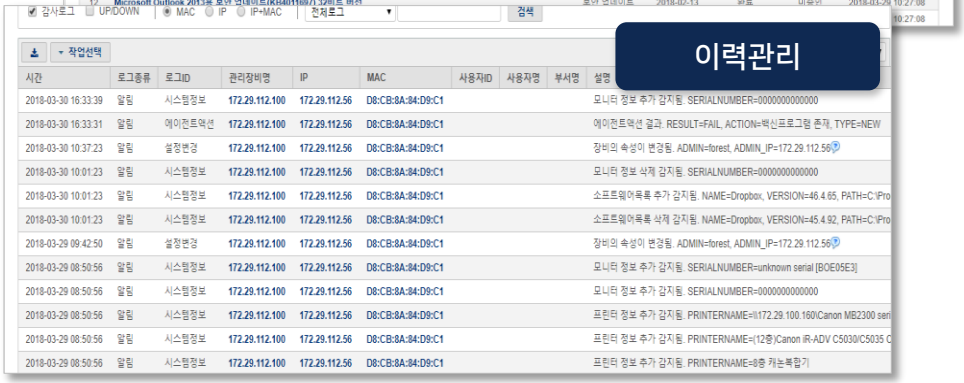




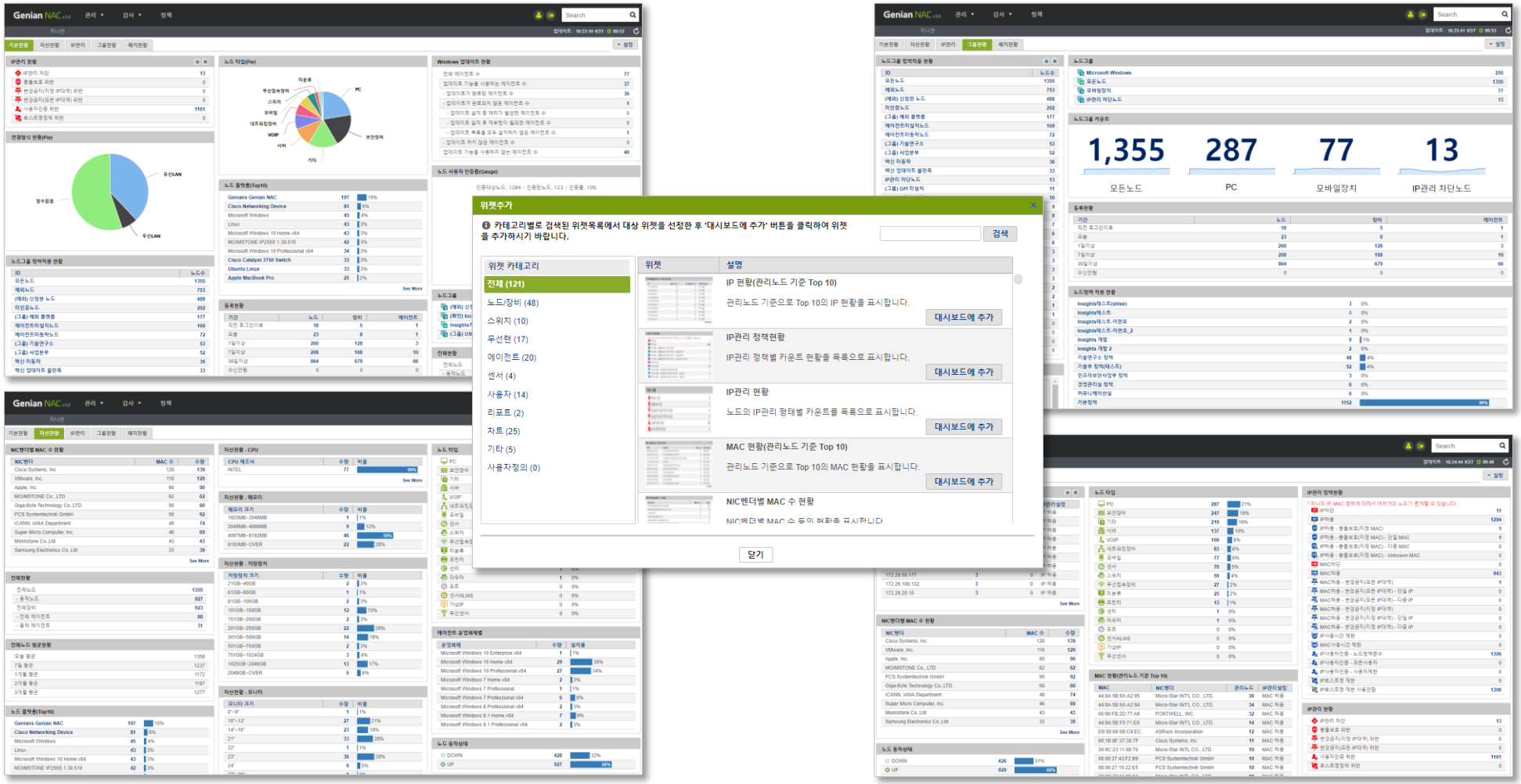






# 가시성 (3/3)

## Dashboard를 통한 다양한 통계, 상태 등의 현황 파악 용이



# 분류 (1/2)

## 다양한 분류 조건 제공(Dynamic Classification)

### 분류 조건


### 그룹 조건 sample

| |
|---|
| IP관리 / 상태 / **차단됨** |
| 플랫폼 / 감지된 플랫폼에 문자열 포함하면 / **Microsoft Windows** |
| 장비내 무선랜 / 무선랜그룹에 속하는 AP가 존재하면 / |
| 접속AP / 무선랜그룹에 속하면 / |
| USB 장치 정보 / 장치명이 문자열을 포함하면 / **WebCam** |
| 구입가격 / 보다 비싸면 / **1000000** |
| 업/다운상태 / 상태값 / **UP** |
| 노드타입 / 감지된 노드타입이 같으면 / **모바일** |
| 인증사용자 / 인증상태 / **인증되지 않음** |
| 백신정보 / 최근검사 시각이 보다 이내이면 / **1 주, 백신명=** |
| 백신정보 / 최근검사 시각이 보다 오래되면 / **1 주, 백신명=** |
| 백신정보 / 백신정보 존재여부 / **존재안함** |
| 백신정보 / 실시간검사 / **사용안함, 백신명=** |
| 백신정보 / 실시간검사 / **사용함, 백신명=** |
| 백신정보 / 패턴날짜가 보다 이내이면 / **1 주, 백신명=** |
| 백신정보 / 패턴날짜가 보다 오래되면 / **1 주, 백신명=** |
| 시스템사용자계정 / 비밀번호없는 로그인된 계정 존재 / |
| 에이전트상태 / 설치상태 / **설치됨** |
| 에이전트상태 / 동작상태 / **Down** |
| 노드그룹 / 속하면 / **Microsoft Windows**<br>에이전트상태 / 설치상태 / **설치안됨** |
| 위험감지 / 노드에 감지된 위험이 / **감지되면** |
| 시스템 / Windows 방화벽 / **사용안함** |

# 분류 (2/2)

## 분류된 정보를 볼 수 있는 통계화면 제공

### 에이전트 운영체제 언어별

| 운영체제 언어 | 수량 | 설치율 |
|---|---|---|
| English | 1 | 1% |
| Korean | 79 | 99% |

### 에이전트 운영체제별

| 운영체제 | 수량 | 설치율 |
|---|---|---|
| Microsoft Windows 10 Enterprise x64 | 1 | 1% |
| Microsoft Windows 10 Home x64 | 30 | 38% |
| Microsoft Windows 10 Professional x64 | 25 | 31% |
| Microsoft Windows 7 Home x64 | 2 | 3% |
| Microsoft Windows 7 Professional | 1 | 1% |
| Microsoft Windows 7 Professional x64 | 7 | 9% |
| Microsoft Windows 8 Professional x64 | 2 | 3% |
| Microsoft Windows 8.1 Home x64 | 6 | 8% |
| Microsoft Windows 8.1 Professional x64 | 2 | 3% |

### IP관리 정책현황

* 하나의 IP, MAC 정책에 대해서 여러개의 노드가 존재할 수 있습니다.

| | |
|---|---|
| IP차단 | 8 |
| IP허용 | 1323 |
| IP허용 - 충돌보호(지정 MAC) | 1 |
| IP허용 - 충돌보호(지정 MAC) - 단일 MAC | 1 |
| IP허용 - 충돌보호(지정 MAC) - 다중 MAC | 0 |
| IP허용 - 충돌보호(지정 MAC) - Unknown MAC | 0 |
| MAC차단 | 0 |
| MAC허용 | 955 |
| MAC허용 - 변경금지(모든 IP대역) | 1 |
| MAC허용 - 변경금지(모든 IP대역) - 단일 IP | 0 |
| MAC허용 - 변경금지(모든 IP대역) - 다중 IP | 0 |
| MAC허용 - 변경금지(지정 IP대역) | 0 |
| MAC허용 - 변경금지(지정 IP대역) - 단일 IP | 0 |
| MAC허용 - 변경금지(지정 IP대역) - 다중 IP | 0 |
| IP사용시간 제한 | 0 |

### IP관리 현황

| | |
|---|---|
| IP관리 차단 | 10 |
| 충돌보호 위반 | 0 |
| 변경금지(지정 IP대역) 위반 | 0 |
| 변경금지(모든 IP대역) 위반 | 0 |
| 사용자인증 위반 | 1191 |
| 호스트명정책 위반 | 0 |

### 노드 타입

| | | |
|---|---|---|
| PC | 288 | 21% |
| 기타 | 258 | 19% |
| 보안장비 | 232 | 17% |
| 서버 | 121 | 9% |
| VOIP | 112 | 8% |
| 네트워킹장비 | 84 | 6% |
| 모바일 | 73 | 5% |
| 센서 | 70 | 5% |
| 스위치 | 58 | 4% |
| 미분류 | 39 | 3% |
| 무선접속장비 | 31 | 2% |
| 프린터 | 13 | 1% |
| 센터 | 1 | 0% |
| 라우터 | 1 | 0% |
| 포트 | 0 | 0% |
| 센서ALIAS | 0 | 0% |
| 가상IP | 0 | 0% |
| 무선센서 | 0 | 0% |

### 제어정책 적용 현황

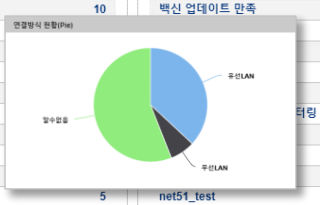
| | | |
|---|---|---|
| HDH_netctrl_test | 0 | 0% |
| 예외허용 | 1012 | 77% |
| 디펜더 미동작 차단 | 3 | 0% |
| 고위험노드 차단 | 0 | 0% |
| IP관리 차단 | 0 | 0% |
| 에이전트미설치차단 | 26 | 2% |
| 미인증차단 | 27 | 2% |
| GPI 미설치 차단 | 1 | 0% |
| 에이전트미동작차단 | 0 | 0% |
| 패치상태불만족차단 | 0 | 0% |
| 백신상태불만족차단 | 0 | 0% |
| 기본정책 | 241 | 18% |

### 등록현황

| 기간 | 노드 | 장비 | 에이전트 |
|---|---|---|---|
| 직전 로그인이후 | 22 | 2 | 1 |
| 오늘 | 51 | 11 | 2 |
| 1일이상 | 157 | 43 | 4 |
| 7일이상 | 328 | 197 | 10 |
| 30일이상 | 845 | 684 | 64 |
| 수신안됨 | 0 | 0 | 0 |

### 노드그룹 정책적용 현황

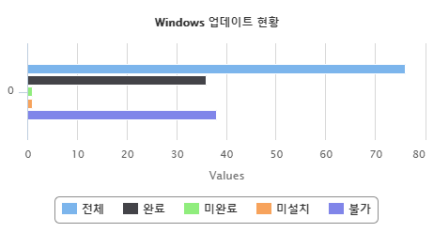
| ID | 노드수 |
|---|---|
| 모든노드 | 1381 |
| 예외노드 | 725 |
| (예외) 신청한 노드 | 455 |
| 미인증노드 | 205 |
| 에이전트미설치노드 | 169 |
| (그룹) 예외 플랫폼 | 162 |
| 에이전트미동작노드 | 57 |
| (그룹) 기술연구소 | 49 |
| (그룹) 사업본부 | 48 |
| 백신 미동작 | 40 |
| 백신 업데이트 불만족 | 37 |
| IP관리 차단노드 | 10 |
| Insights개발(이민상1) | |
| (그룹) GPI 미설치 | |
| 백신 실시간검사 미사용 | |
| 패치상태불만족노드 | |
| (예외) 임시 예외노드 | |
| Defender 모니터링 그룹 | |
| PC | |
| (그룹) 경영관리실 | |
| (그룹) 커뮤니케이션실 | 5 |
| 백신 미존재 | 4 |
| (그룹) 신규사업TFT | 3 |
| Insights테스트(shlee) | 3 |
| (예외) 빌드서버 | 2 |
| Insights개발(이민상2) | 2 |
| Insights개발(이현호) | 2 |




### 노드그룹 정책미적용

| ID | 노드수 |
|---|---|
| (확인) local | 1381 |
| (그룹) USB차단 | 1379 |
| 동작노드 | 903 |
| 컴플라이언스 위반노드 | 474 |
| 위험감지노드 | 425 |
| Microsoft Windows | 258 |
| 에이전트 설치노드 | 113 |
| 백신 실시간검사 사용 | 111 |
| (그룹) 국보연 테스트_BIOS_정보수집 | 108 |
| (그룹) 국보연 테스트_BIOS_Password | 108 |
| (현황) GPI 설치현황 | 102 |
| 백신 업데이트 만족 | 78 |
| | 73 |
| | 66 |
| | 38 |
| | 16 |
| 터링 | 8 |
| | 7 |
| | 7 |
| | 7 |
| net51_test | 6 |
| v3 설치 여부 확인 | 4 |
| 비밀번호 없는 로그인계정 | 4 |
| 화면보호기 미설정 | 4 |
| net99_test | 3 |
| (그룹) 해외사업부 | 2 |
| (예외) USB차단 예외허용 | 2 |

### Windows 업데이트 현황(차트)




### 노드 태그

| | | |
|---|---|---|
| HDH테스트 | 0 | 0% |
| THREAT | 0 | 0% |
| 고위험 | 1 | 0% |
| 관리자 | 0 | 0% |
| 네트워크차단 | 0 | 0% |
| 악성코드차단 | 0 | 0% |
| 에이전트설치예외 | 7 | 1% |
| 임시예외 | 1 | 0% |
| 장치제어예외 | 1 | 0% |
| 중위험 | 1 | 0% |

# 통제

## 다양한 제어 및 단계적 검증을 통한 보안 강화

### 알림(Alarm)

- 사용자에게 알림
  (차단 웹, 에이전트 팝업, 인스턴스 메시지)
- 관리자에게 알림
  (특정 이벤트 발생 시 SMS, E-mail 발송)
- 특정 로그 외부 전송
  (타 보안 솔루션으로 로그 전송하여 모니터링)

### 차단(Block)

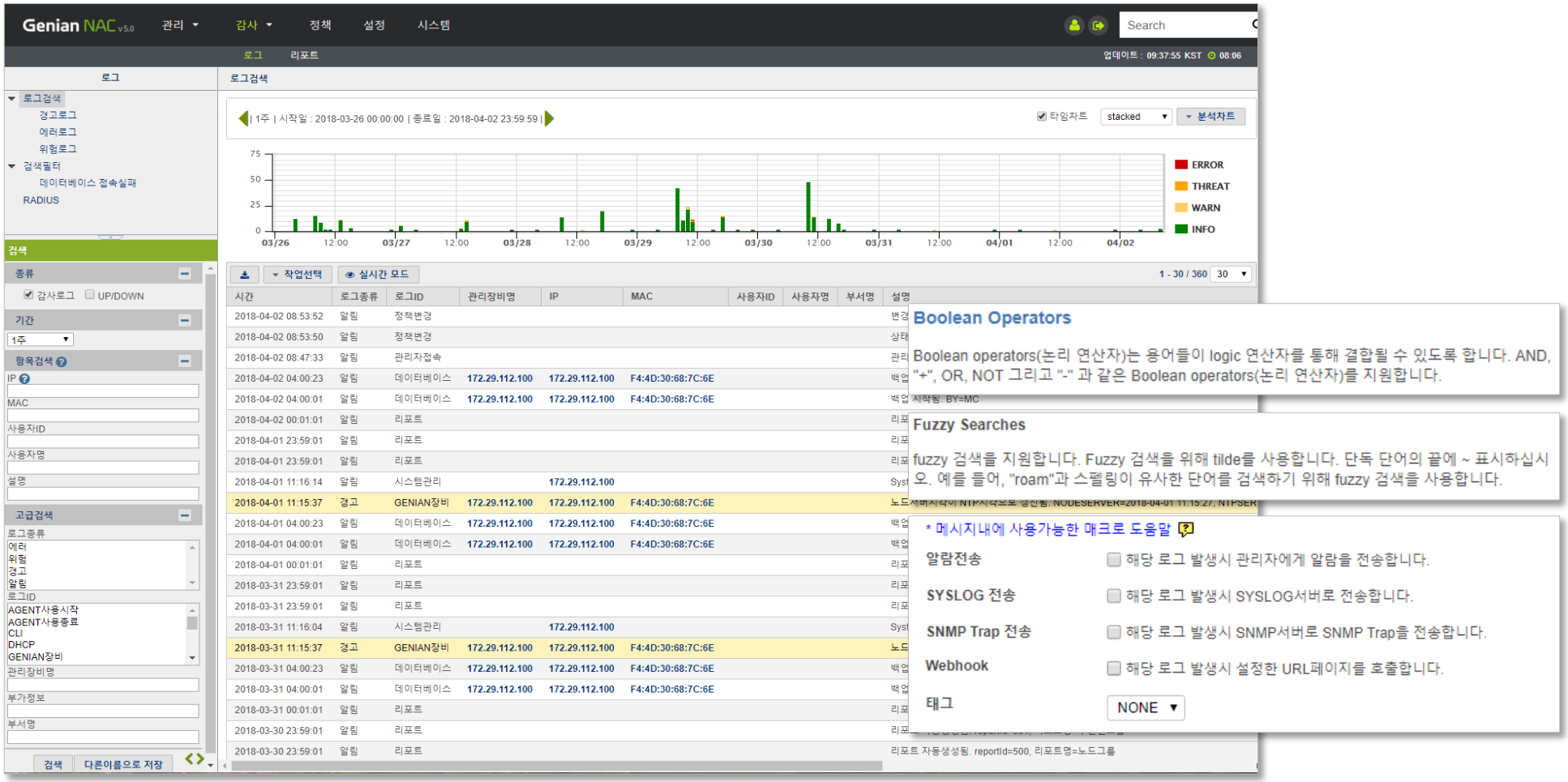
- 조건에 따른 네트워크 차단
  (신규 IP/MAC, 미 인증, 보안 설정 위반 등)
- 특정 프로세스 중지
  (관리자가 지정한 프로세스)
- USB 장치 차단
  (USB 저장 장치 등 강제 Off)

### 교정(Remediation)

- 필수 SW 설치 유도
  (백신, DRM, DLP 등 보안 솔루션 강제 설치)
- 불법 SW 삭제
  (허용되지 않은 특정 SW 강제 삭제)
- 보안 설정 강제화
  (패스워드 설정, 화면보호기 등)

# 리포트 (1/2)

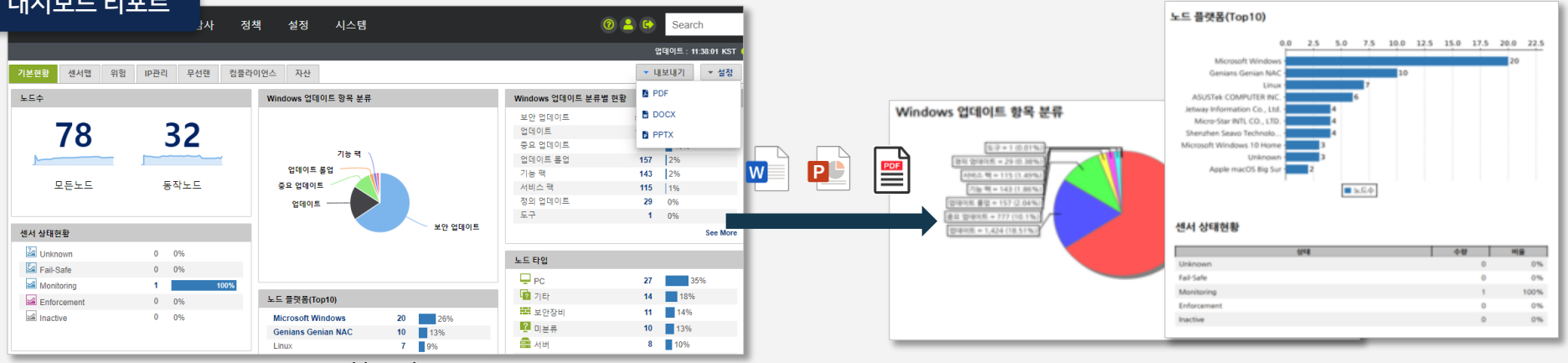
## 감사로그 필터링 & 로그 전송(SMS, E-mail, Syslog, Snmptrap)



# 리포트 (2/2)

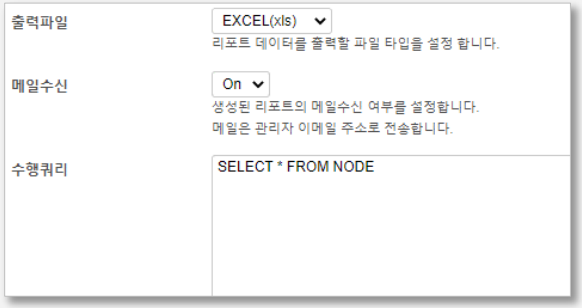
## 대시보드,노드, 쿼리, 로그 Report 제공

### 대시보드 리포트



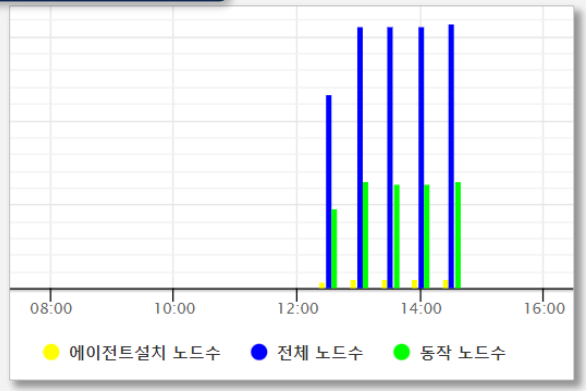

Dashboard

### 쿼리 리포트




※ 쿼리를 통해 추출한 데이터를 Excel형태로 제공
※ 설정한 주기에 따라 관리자에게 E-Mail 송신

### 노드 리포트




※ 설정한 데이터의 기간 별 평균, 최대값 통계 제공

### 로그 리포트

| 이름 | 오늘 | 전일 | 전주 | 전월 | 전일비 | 전주비 | 전월비 |
|---|---|---|---|---|---|---|---|
| 에러 | 8 | 12 | 12 | 0 | -4 | -4 | 8 |
| 위험 | 0 | 0 | 0 | 2 | 0 | 0 | -2 |
| 경고 | 0 | 0 | 0 | 201 | 0 | 0 | -201 |

※ 로그 별 발생 추이 통계 제공

# 기능 요약

## Agent-less

※ Agent 없는 환경에서도 다양한 방식으로 접근제어

| | |
|---|---|
| Platform 분류 | OS(Windows, Linux, Unix, iOS, Android 등), 네트워크 장비, 프린터, 제조사 등 |
| 접근제어 | IP, MAC, PORT, Protocol 별 접근 제어 |
| | Platform 별 접근 제어(OS 및 장치 별) |
| | 시간/요일/기간 접근 제어 |
| | 사용자 별 접근 제어<br>(인증/미 인증, ID, 부서, 직급 등) |
| 네트워크 정보 | IP 관리 (IP/MAC 고정, 변경금지, 충돌보호, 사용시간 등) |
| | 사용자 PC 가 연결된 스위치 및 포트 정보 |
| | Host 명, Domain 명 |
| | PC 동작 유무 판단, PC 열린 포트 정보 |

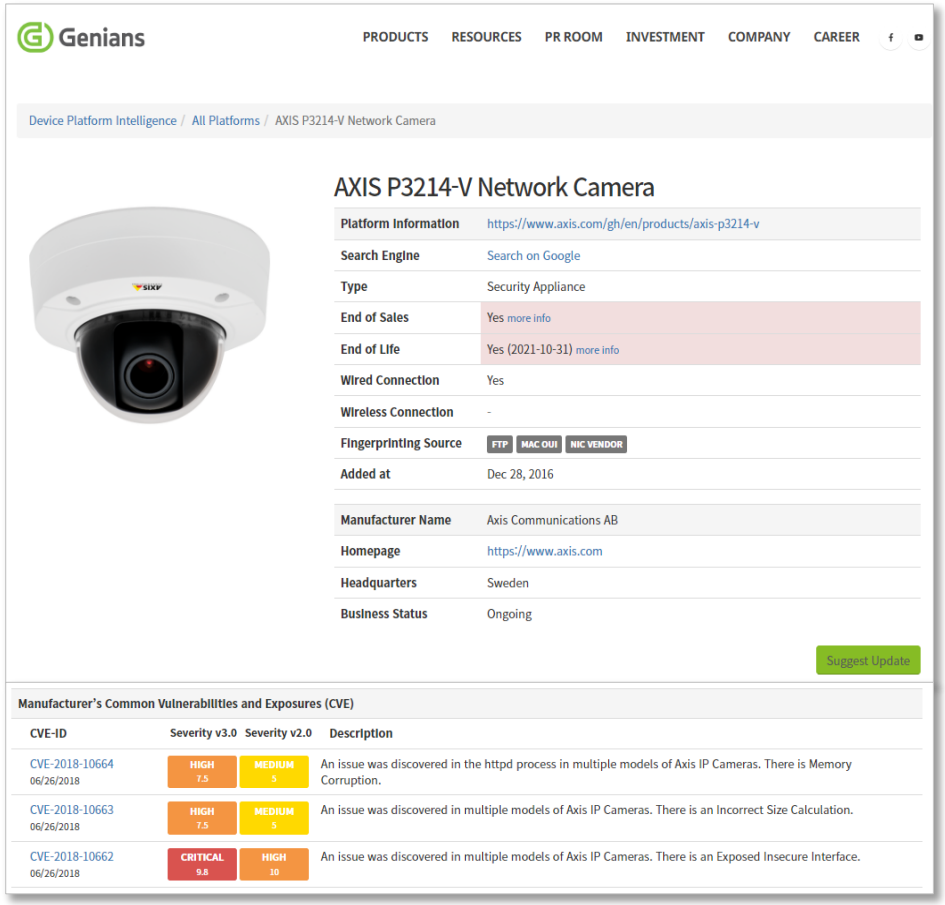
## Agent

| | |
|---|---|
| Windows 패치 | Windows patch(PMS) 기능 제공 |
| 세션제어 | TCP 세션 정보 수집 및 임계치 초과 시 차단 |
| 포트 정보 | 열린 포트, 포트 사용 프로세스, 서비스 정보 |
| 장치 제어 | USB, NIC, Bluetooth, Wifi, Tethering, PC전원 제어 |
| 프로세스 제어 | 특정 프로세스 강제 종료 |
| 백신 연동 | 백신(V3, 바이로봇, 알약)업데이트 및 바이러스 탐지에 대한 네트워크 제어 |
| 소프트웨어 탐지 | 필수 S/W, 불법 S/W 탐지 및 제어 |
| 메시지 전송 | 사용자에게 메시지 전송(공지 및 알림 팝업) |
| 보안 기능 | 윈도우 보안 설정, 자동 실행 제어, 무선랜 제어,<br>호스트명 변경, 화면보호기 제어, 파일배포,<br>계정 취약성 검사 |
| 위 변조 탐지 | IP, MAC clone 탐지/차단 |
| AP 탐지 | 무선 AP 탐지 및 접속 제어 |
| 시스템정보 | PC OS 및 H/W 정보(CPU, MEM, DISK, NIC 등),<br>Hostname 수집 및 제어 |
| OS 업데이트 | OS 자동 업데이트 기능 제공 |
| 장치 제어 | USB, NIC, Bluetooth, Wifi, Tethering |
| 보안기능 | 화면보호기 제어, 에이전트 인증, 공유 폴더 제어,<br>비밀번호 유효성 검사, 파일배포, 방화벽 제어 |

# 제품 특장점

## 단말 플랫폼 인텔리전스(Device Platform Intelligence)

### DPI를 이용한 단말 제조사 및 취약점 정보확인




### DPI가 제공하는 단말 관련 정보

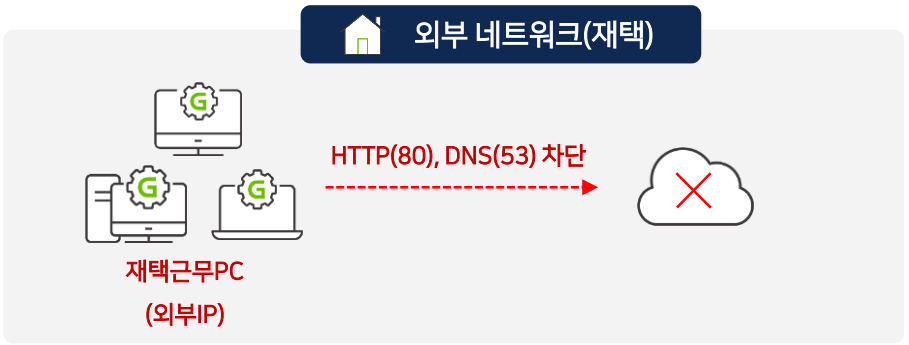
| 구분 | 세부정보 |
|---|---|
| 단말 식별 정보<br>(Device Identity) | · 단말 제조사, 이름, 모델번호<br>· 단말 사진<br>· 네트워크 연결 방식(Wired/Wireless)<br>· 단말 상세 정보 URL |
| 단말 확장 정보<br>(Device Context) | · 제조사 명칭<br>· 제조사 홈페이지 URL<br>· 본사의 위치와 현재 사업 진행 여부<br>· 제품 판매 종료(End of Sales) 여부<br>· 제품 지원 종료(End of Support) 여부<br>· 검색엔진 연결 URL |
| 단말 위협 정보<br>(Device Risk) | · 단말에 알려진 CVE 정보<br>(CVE No. / Severity / Description 등)<br>· 제조사에 알려진 CVE 정보<br>(CVE No. / Severity / Description 등) |

# 제품 특장점

## SAML (G-Suite, okta 인증 연동)

# 제품 특장점

## 업무용PC 외부 사용 제어


아웃바운드 규칙

| 이름 | 그룹 | 프로필 | 사용 | 작업 | 다시 정의 |
|---|---|---|---|---|---|
| nProtect Online Security Updater | | 모두 | 예 | 허용 | 아니요 |
| Wizvera-Delfino-G3-out | | 모두 | 예 | 허용 | 아니요 |
| Wizvera-Veraport-G3-out | | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.BingWeather_4.46.23383.0... | @{Microsoft.BingWeather_... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.DesktopAppInstaller_1.4.31... | @{Microsoft.DesktopAppIn... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.GetHelp_10.2011.33361.0_... | @{Microsoft.GetHelp_10.20... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.Getstarted_9.13.33161.0_x... | @{Microsoft.Getstarted_9.1... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.Messaging_4.1901.10241.... | @{Microsoft.Messaging_4.1... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.Microsoft3DViewer_7.2010... | @{Microsoft.Microsoft3DVi... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.MicrosoftEdge_44.18362.4... | @{Microsoft.MicrosoftEdge... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.MicrosoftStickyNotes_3.8.8... | @{Microsoft.MicrosoftStick... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.MixedReality.Portal_2000.2... | @{Microsoft.MixedReality.P... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.MSPaint_6.2009.30067.0_x... | @{Microsoft.MSPaint_6.20... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.OneConnect_5.2011.3081.... | @{Microsoft.OneConnect_5... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.People_10.1909.12456.0_x... | @{Microsoft.People_10.190... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.PPIProjection_10.0.18362.... | @{Microsoft.PPIProjection_... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.StorePurchaseApp_12011.... | @{Microsoft.StorePurchase... | 모두 | 예 | 허용 | 아니요 |

아웃바운드 규칙

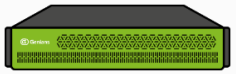
| 이름 | 그룹 | 프로필 | 사용 | 작업 | 다시 정의 |
|---|---|---|---|---|---|
| TCP/80 차단 | | 모두 | 예 | 거부 | 아니요 |
| UDP/53 차단 | | 모두 | 예 | 거부 | 아니요 |
| nProtect Online Security Updater | | 모두 | 예 | 허용 | 아니요 |
| Wizvera-Delfino-G3-out | | 모두 | 예 | 허용 | 아니요 |
| Wizvera-Veraport-G3-out | | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.BingWeather_4.46.23383.0... | @{Microsoft.BingWeather_... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.DesktopAppInstaller_1.4.31... | @{Microsoft.DesktopAppIn... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.GetHelp_10.2011.33361.0_... | @{Microsoft.GetHelp_10.20... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.Getstarted_9.13.33161.0_x... | @{Microsoft.Getstarted_9.1... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.Messaging_4.1901.10241.... | @{Microsoft.Messaging_4.1... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.Microsoft3DViewer_7.2010... | @{Microsoft.Microsoft3DVi... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.MicrosoftEdge_44.18362.4... | @{Microsoft.MicrosoftEdge... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.MicrosoftStickyNotes_3.8.8... | @{Microsoft.MicrosoftStick... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.MixedReality.Portal_2000.2... | @{Microsoft.MixedReality.P... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.MSPaint_6.2009.30067.0_x... | @{Microsoft.MSPaint_6.20... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.OneConnect_5.2011.3081.... | @{Microsoft.OneConnect_5... | 모두 | 예 | 허용 | 아니요 |
| @{Microsoft.People_10.1909.12456.0_x... | @{Microsoft.People_10.190... | 모두 | 예 | 허용 | 아니요 |

※ Windows Defender 방화벽 제어를 통한 외부 네트워크 사용 시 관리자가 설정한 커스텀 규칙 적용

# 제품 특장점

## 외부 DB서버와 연동을 통한 가시성 확보

### DB 연동 지원 범위



NAC
Policy Server

- ORACLE
- MYSQL
- MSSQL/Sybase
- IBM DB2
- Tibero
- Altibase
- PostgreSQL
- LDAP
- CSV
- CSV(Upload)
- CUBRID
- Google G Suite
- REST API Server

### 연동을 통한 가시성 확보

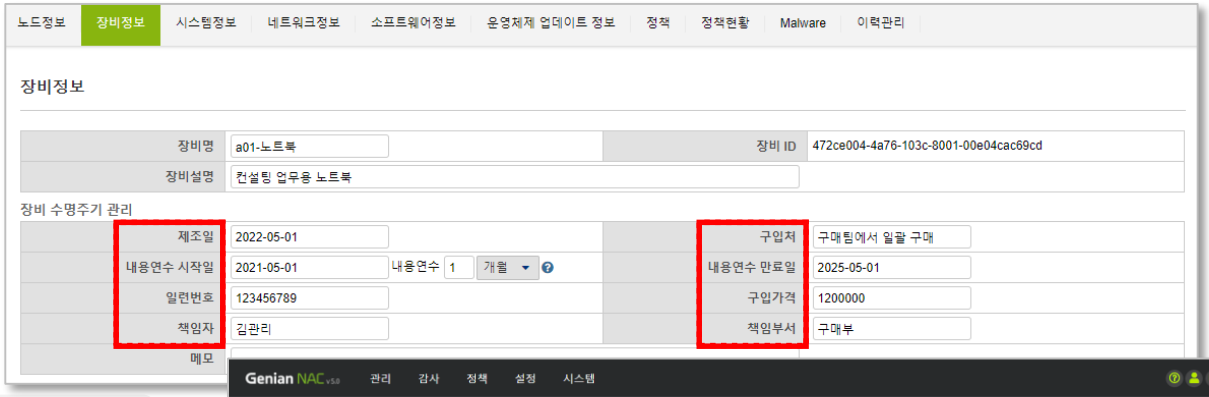

기존에 운영 중인 시스템의 데이터를 연동하여 추가적인 가시성 확보

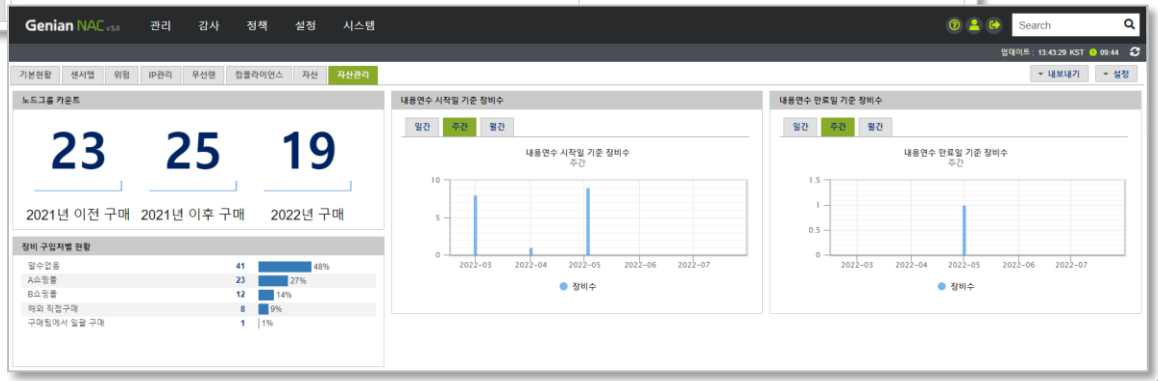
# 제품 특장점

## 장비 수명주기 관리

### 연동을 통한 가시성 확보


장비정보
장비명
장비설명
제조일
구입처
내용연수 시작일
내용연수 만료일
일련번호
구입가격
책임자
책임부서
메모




제조일, 내용연한, 가격, 책임부서 등의 정보를 입력하여 그룹을 설정할 수 있으며, 대시보드에서 현황 관리 및 연한이 넘은 장치에 대해서 사용자/관리자에 알림 기능을 제공합니다.

# 제품 특장점

## 사용자 PC 의 안정성을 보장하는 Agent

| OS | PT | RA | 액션명 ↑ | 플러그인명 |
|---|---|---|---|---|
| | | | ARP 관리 | ARP 관리 |
| | | | DNS 제어 | DNS 제어 |
| | | | IE보안옵션 제어 | 웹브라우저 옵션 제어 |
| | | | Malware Detector | Malware Detector |
| | | | TCP세션검사 | TCP세션검사 |
| | | | Windows 방화벽 제어 | Windows 방화벽 제어 |
| | | | Windows 보안설정 | Windows 보안설정 |
| | | | Windows 업데이트 | Windows 업데이트 |
| | | | WMI정보수집 | WMI정보수집 |
| | | | 공유프로그램 미존재 | 수행조건만 검사 |
| | | | 네트워크 공유폴더 | 네트워크 공유폴더 |
| | | | 네트워크 트래픽 제어 | 네트워크 트래픽 제어 |
| | | | 네트워크정보 수집 | 네트워크정보 수집 |
| | | | 메신져프로그램 미존재 | 수행조건만 검사 |
| | | | 모니터정보 수집 | 모니터정보 수집 |
| | | | 모양 및 개인설정 | 모양 및 개인설정 |
| | | | 무선 연결 관리자 | 무선 연결 관리자 |
| | | | 무선랜제어 | 무선랜제어 |
| | | | 무선랜제어(외부) | 무선랜제어 |
| | | | 백신정보 수집 | 백신정보 수집 |
| | | | 백신프로그램 존재 | 수행조건만 검사 |
| | | | 비밀번호유효성검사 | 비밀번호유효성검사 |

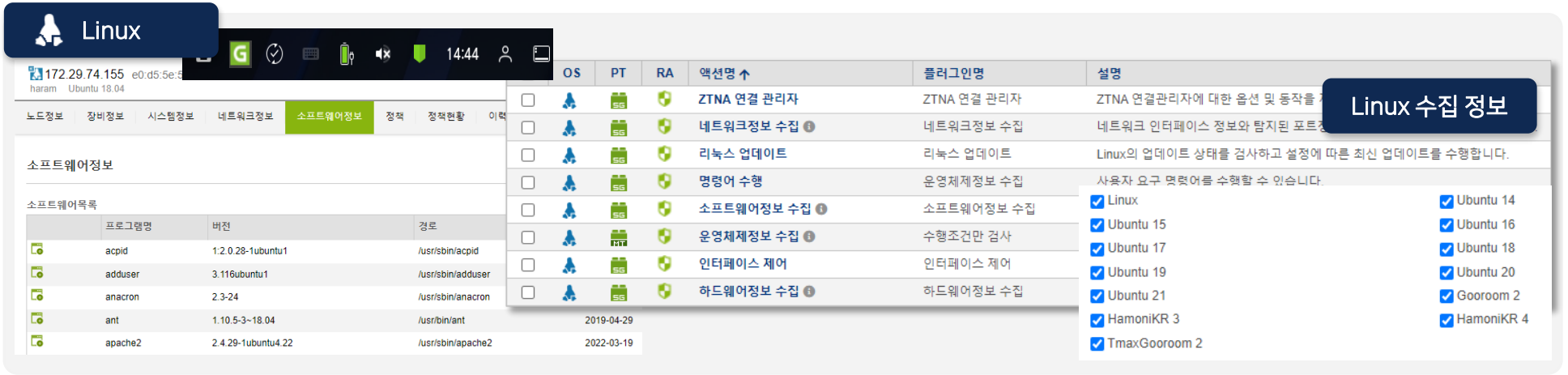
- 모든 기능 플러그인 형태로 제공하여 선택/추가 용이함
- 선택적 기능 사용으로 리소스 사용 최소화
- Non-Kernel 기반의 동작(OS 충돌 위험 최소화)
- 1,300곳 이상의 고객사에서 검증된 안정성
  (최소 150만 대 이상)

# 제품 특장점

## macOS/ Linux Agent

### macOS


### Linux



# 제품 특장점

## USB 장치 정보 자동수집 및 조건 설정 그룹 생성

수집된 USB 정보 확인

노드정보 | 장비정보 | 시스템정보 | 네트워크정보 | 소프트웨어정보 | 운영체제 업데이트 정보 | 정책 | 정책현황 | Malware | 이력관리

USB 정보

| 클래스명 | 장치명 | 제조사 | 모델명 | 시리얼 | 상태 |
|---|---|---|---|---|---|
| Bluetooth | AirPods Pro YA - Find My | | | | 사용 |
| Bluetooth | Microsoft Sculpt Touch Mouse | | | | 사용 |
| Bluetooth | iPhone | | | | 사용 |
| 기타 장치 | Wireless iAP | | | | 사용 |
| Bluetooth | 서비스 검색 서비스 | | | | 사용 |
| 사운드, 비디오 및 게임 컨트롤러 | iPhone A2DP SNK | | | | 사용 |
| 사운드, 비디오 및 게임 컨트롤러 | AirPods Pro YA - Find My Stereo | | | | 사용 |
| Bluetooth | iPhone Avrcp 전송 | | | | 사용 |
| Bluetooth | AirPods Pro YA - Find My Avrcp 전송 | | | | 사용 |
| Bluetooth | 개인 영역 네트워크 NAP 서비스 | | | | 사용 |
| Bluetooth | 전화 번호부 액세스 PSE 서비스 | | | | 사용 |
| 기타 장치 | MAP MAS-iOS | | | | 사용 |
| Bluetooth | 장치 식별 서비스 | | | | 사용 |
| 기타 장치 | GATT | | | | 사용 |
| 기타 장치 | Wireless iAP v2 | | | | 사용 |
| 기타 장치 | AAP Server | | | | 사용 |
| 사운드, 비디오 및 게임 컨트롤러 | iPhone Hands-Free HF Audio | | | | 사용 |
| 사운드, 비디오 및 게임 컨트롤러 | AirPods Pro YA - Find My Hands-Free AG Audio | | | | 사용 |
| Bluetooth | 일반 액세스 프로필 | | | | 사용 |
| Bluetooth | 일반 특성 프로필 | | | | 사용 |

조건설정

항목: USB 장치 정보

조건: 특정 클래스가 존재하면

설정

설정메모

[설정내용] 클래스가 존재하면

- 특정 클래스가 존재하면
- 특정 클래스가 존재하지 않으면
- 장치명이 문자열을 포함하면
- 모델명이 문자열을 포함하면
- 특정 클래스에 사용중인 장치가 존재하면
- 특정 클래스에 사용중지된 장치가 존재하면
- 사용중인 장치의 이름이 문자열을 포함하면
- 사용중이지 않는 장치의 이름이 문자열을 포함하면

다양한 조건 설정을 통해 USB 장치 사용자 현황 확인

| ID | 노드수 | 사용 | 연산 | 설정 |
|---|---|---|---|---|
| 특정 USB장치 사용자 | 1 | ☑ | OR | USB 장치 정보 / 특정 클래스가 존재하면 / 카메라<br>USB 장치 정보 / 장치명이 문자열을 포함하면 / SanDisk |

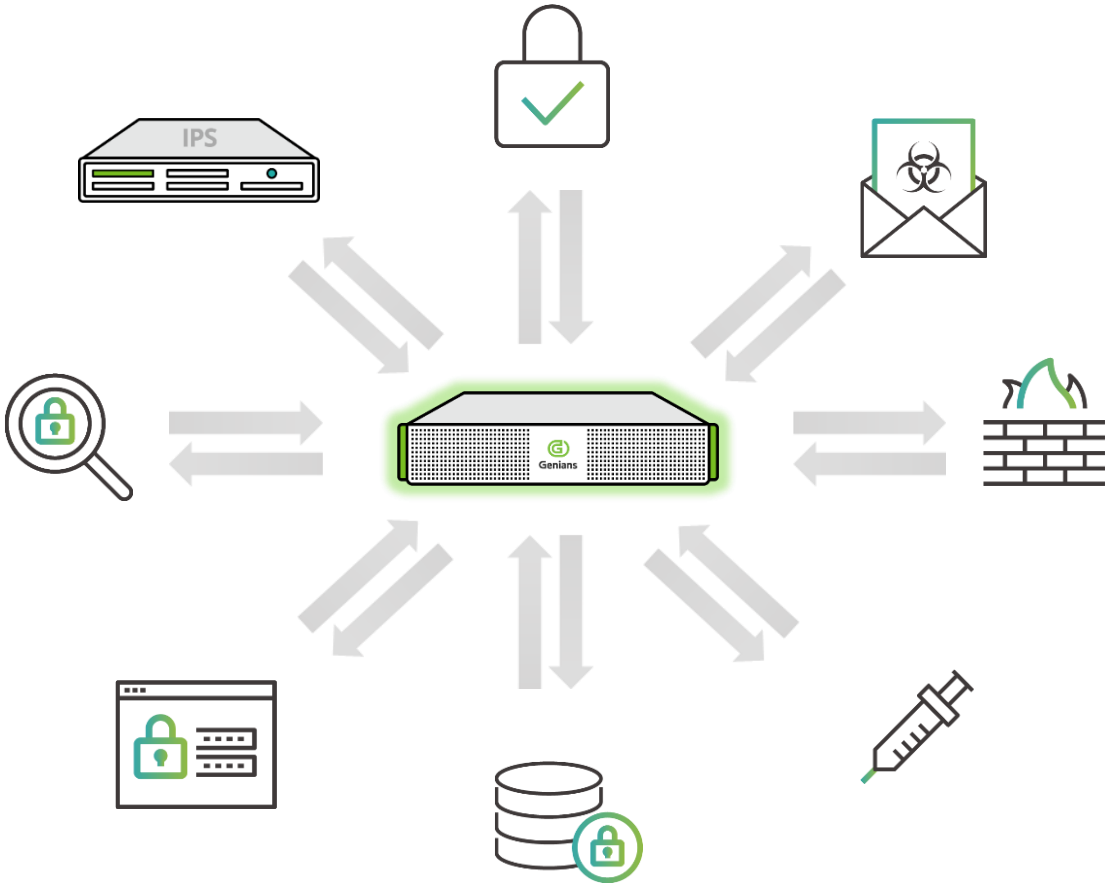
노드그룹: 특정 USB장치 사용자

작업선택 | NodeGroup = '특정 USB장치 사용자' | 검색 | 1 - 1 / 1 | 50

| NT AG SS | 위험 | 동작 | 동작상태차트 | IP주소 | MAC주소 | 정책 | 제어정책 | 호스트명(이름) | 플랫폼 |
|---|---|---|---|---|---|---|---|---|---|
| | | | | 172.30.100.190 | 00:E0:4C:68:00:29 | DHCP | 기본정책 | YOONA | Microsoft Windows 10 Home x64 |

# 제품 특장점

## Security Ecosystem




### 다양한 보안 시스템과의 연동 제공

Syslog
- 송/수신 기능
- 로그 수신 후 해당 IP 에 대한 제어

Snmptrap
- 송/수신 기능
- 로그 수신 후 해당 IP 에 대한 제어

Rest API
- 타 그룹웨어와의 연동을 위한 유연한 방식
- 신청/결재 시스템 연동

DB 연동
- DB 연동으로 추가적인 정보 제공

# 도입 효과

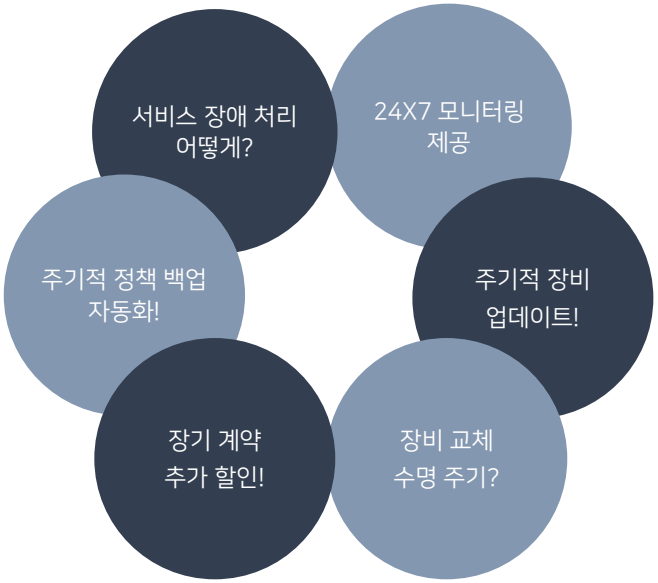
## 가시성 확보와 다양한 형태의 제어, 단계적 검증을 통한 내부 네트워크 보안 강화

관리의 편리성과 보안 강화

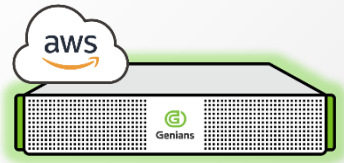
1. 네트워크 내의 단말기 현황 파악 및 관리
2. 보안 정책 미 준수 단말에 대한 네트워크 차단 및 필수 SW 설치 강제화
3. 인증을 통한 IP 실명제

# 제품 특징 비교

## Genians Hosted Solution (SaaS)




### Genian Cloud NAC (SaaS)




Cloud Hybrid 설치

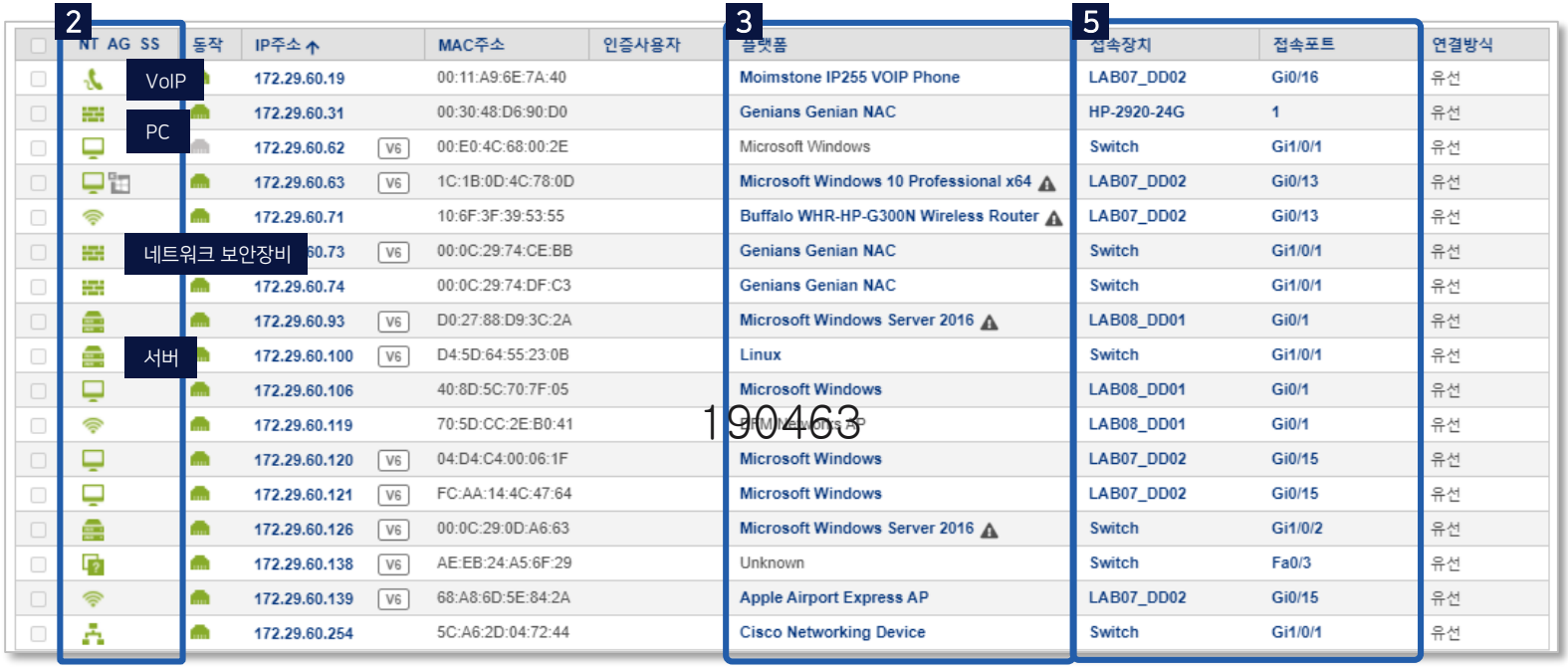
- 24x7x365 장비 동작 모니터링 수행
- EC2 인스턴스 상태 실시간 모니터링
- 개별 POD 생성 운영
  - EC2 장애 발생시 별도 영역의 EC2로 자동전환
- Managed Service 를 통한  서비스 대응 시간 단축
- 고객 인스턴스 정기적인 백업 (AWS S3 & Glacier)
- 장애 시 자동 복구기능을 통해 서비스 지연 최소화
- 장치 구성간 안전한 암호화 통신 (TLS 1.3)
- 최신 릴리즈 버전 / 펌웨어 상시 업데이트 제공

03.

# 사용자 스토리

# 관리자 영역

## Phase: 가시성 확보 → 비인가단말제어 → 인증 → 무결성검사




| 순 서 | 설 명 | |
|---|---|---|
| 1 | 차단센서 물리적인 설치 완료 | 물리적인 장비 설치가 끝나면 네트워크 스캔을 시작하고 수집된 정보를 기반으로 타입과 플랫폼을 분류합니다. |
| 2 | 각 단말의 종류(PC/ 프린터/ 서버/ 모바일 등) 분류 | |
| 3 | 호스트명/ OS 정보 수집 | |
| 4 | NAC 사용자 인증 전단계로 사용자 정보는 확인 할 수 없음 | |
| 5 | 스위치 SNMP 연동(SNMP community)을 통해 위치 정보 확인 | |

# 관리자 영역

Phase: 가시성 확보 → 비인가단말제어 → 인증 → 무결성검사

## “보여야 알 수 있고 알아야 관리할 수 있다”

NC250

- ✓ 1분이면 안방까지 뚫린다 … 사물인터넷 파고든 해킹 (KBS)
- ✓ 안방 CCTV를 누군가 훔쳐본다…스마트 홈 파고드는 ‘IoT 해킹’ (동아일보)
- ✓ IP 카메라 해킹해 남의 집 안방 훔쳐본 외국인 강사 벌금형 (연합뉴스)
- ✓ 홈 IoT 도어락 해킹해 10초만에 딸깍 (보안뉴스)
- ✓ ‘실종된 사생활’…IoT 해킹경고 (디지털타임스)
- ✓ “현관문 따고 집안 훔쳐보고”…’IoT 60%’ 스마트홈 해킹 ‘숭숭’ (KBS)

**Platform's Common Vulnerabilities and Exposures (CVE)**

| CVE-ID | Severity v3.0 | Severity v2.0 | Description |
|---|---|---|---|
| CVE-2017-10796<br>07/02/2017 | MEDIUM | LOW | On TP-Link NC250 devices with firmware through 1.2.1 build 170515, anyone can view video and audio without authentication via an rtsp://admin@yourip:554/h264_hd.sdp URL |

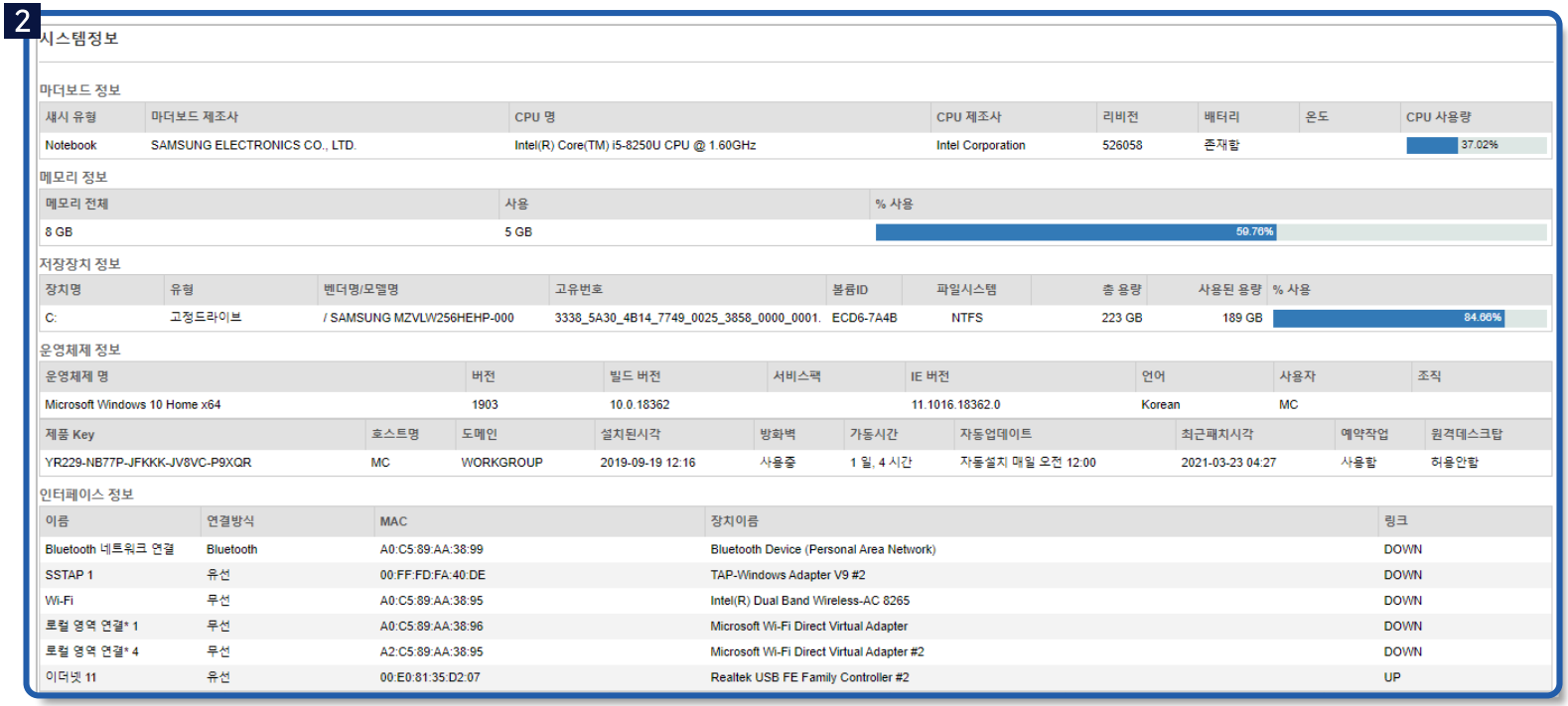
1

비인가 사용자가 비디오 파일, 오디오 파일에 접근할 수 있는 취약점

# 관리자 영역

## Phase: 가시성 확보 → 비인가단말제어 → 인증 → 무결성검사

2



시스템정보

마더보드 정보

| 섀시 유형 | 마더보드 제조사 | CPU 명 | CPU 제조사 | 리비전 | 배터리 | 온도 | CPU 사용량 |
|---|---|---|---|---|---|---|---|
| Notebook | SAMSUNG ELECTRONICS CO., LTD. | Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz | Intel Corporation | 526058 | 존재함 | | 37.02% |

메모리 정보

| 메모리 전체 | 사용 | % 사용 |
|---|---|---|
| 8 GB | 5 GB | 59.76% |

저장장치 정보

| 장치명 | 유형 | 벤더명/모델명 | 고유번호 | 볼륨ID | 파일시스템 | 총 용량 | 사용된 용량 | % 사용 |
|---|---|---|---|---|---|---|---|---|
| C: | 고정드라이브 | / SAMSUNG MZVLW256HEHP-000 | 3338_5A30_4B14_7749_0025_3858_0000_0001. | ECD6-7A4B | NTFS | 223 GB | 189 GB | 84.66% |

운영체제 정보

| 운영체제 명 | 버전 | 빌드 버전 | 서비스팩 | IE 버전 | 언어 | 사용자 | 조직 |
|---|---|---|---|---|---|---|---|
| Microsoft Windows 10 Home x64 | 1903 | 10.0.18362 | | 11.1016.18362.0 | Korean | MC | |

| 제품 Key | 호스트명 | 도메인 | 설치된시각 | 방화벽 | 가동시간 | 자동업데이트 | 최근패치시각 | 예약작업 | 원격데스크탑 |
|---|---|---|---|---|---|---|---|---|---|
| YR229-NB77P-JFKKK-JV8VC-P9XQR | MC | WORKGROUP | 2019-09-19 12:16 | 사용중 | 1 일, 4 시간 | 자동설치 매일 오전 12:00 | 2021-03-23 04:27 | 사용함 | 허용안함 |

인터페이스 정보

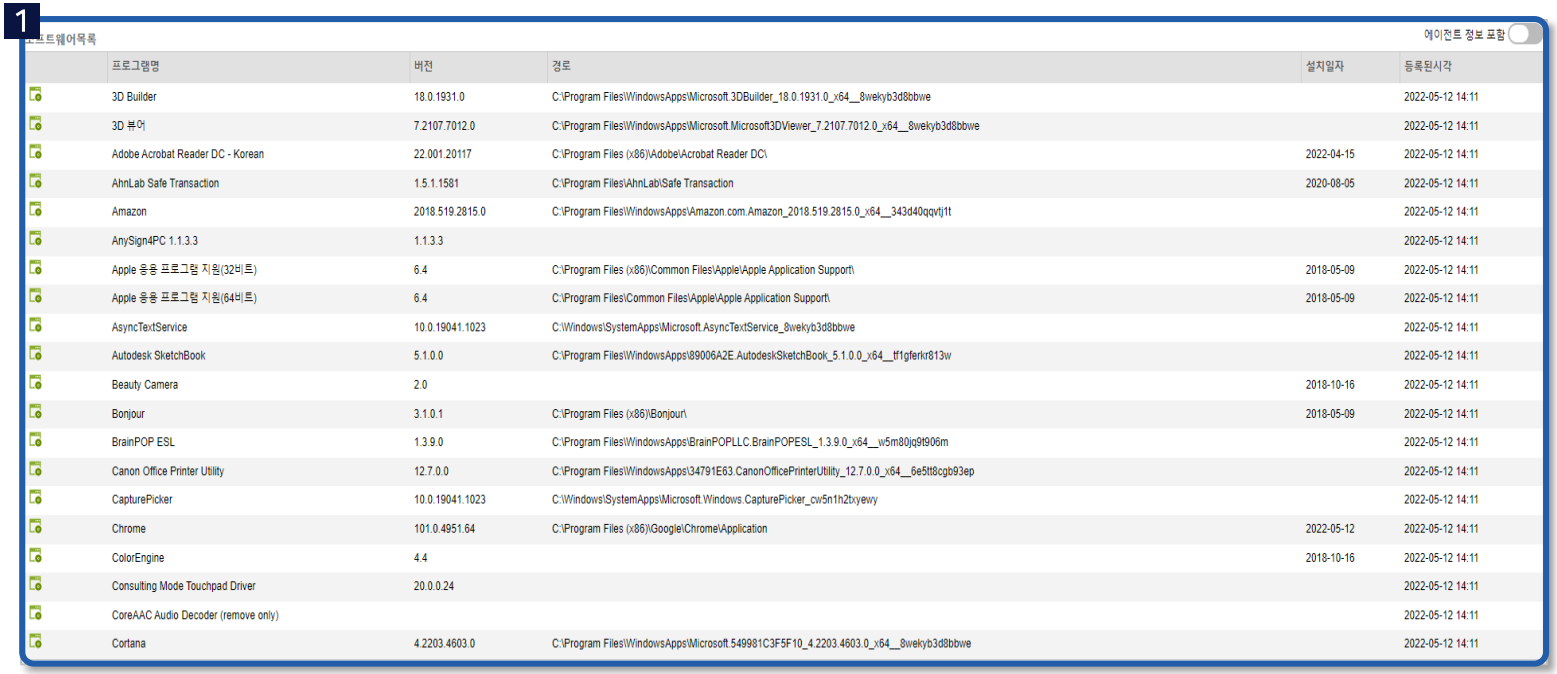
| 이름 | 연결방식 | MAC | 장치이름 | 링크 |
|---|---|---|---|---|
| Bluetooth 네트워크 연결 | Bluetooth | A0:C5:89:AA:38:99 | Bluetooth Device (Personal Area Network) | DOWN |
| SSTAP 1 | 유선 | 00:FF:FD:FA:40:DE | TAP-Windows Adapter V9 #2 | DOWN |
| Wi-Fi | 무선 | A0:C5:89:AA:38:95 | Intel(R) Dual Band Wireless-AC 8265 | DOWN |
| 로컬 영역 연결* 1 | 무선 | A0:C5:89:AA:38:96 | Microsoft Wi-Fi Direct Virtual Adapter | DOWN |
| 로컬 영역 연결* 4 | 무선 | A2:C5:89:AA:38:95 | Microsoft Wi-Fi Direct Virtual Adapter #2 | DOWN |
| 이더넷 11 | 유선 | 00:E0:81:35:D2:07 | Realtek USB FE Family Controller #2 | UP |

| 순 서 | 설 명 | |
|---|---|---|
| 1 | 설치된 단말의 시스템 정보 수집 사전 배포 | 기 운영 중인 배포 시스템이 있다면 NAC Agent를 사전배포(강제화 전)하여 단말의 가시성을 확보할 수 있습니다. |
| 2 | 각 단말의 종류(PC/ 프린터/ 서버/ 모바일 등) 분류<br>- 하드웨어 정보: 마더보드/ CPU/ 메모리/ 저장장치/ 인터페이스 등 정보수집<br>- 운영체제 정보: 운영체제/버전/빌드 버전/언어 등 정보수집<br>- 공유폴더/ 화면보호기/ 윈도우 방화벽/ 호스트명 변경(인사DB 활용)<br>- 사용자계정 정보: 비밀번호 규칙(변경주기)/ 계정타입(관리자, 사용자)에 따른 제어 | |

# 관리자 영역

## Phase: 가시성 확보 → 비인가단말제어 → 인증 → 무결성검사

1



소프트웨어목록

에이전트 정보 포함

| | 프로그램명 | 버전 | 경로 | 설치일자 | 등록된시각 |
|---|---|---|---|---|---|
| | 3D Builder | 18.0.1931.0 | C:\Program Files\WindowsApps\Microsoft.3DBuilder_18.0.1931.0_x64__8wekyb3d8bbwe | | 2022-05-12 14:11 |
| | 3D 뷰어 | 7.2107.7012.0 | C:\Program Files\WindowsApps\Microsoft.Microsoft3DViewer_7.2107.7012.0_x64__8wekyb3d8bbwe | | 2022-05-12 14:11 |
| | Adobe Acrobat Reader DC - Korean | 22.001.20117 | C:\Program Files (x86)\Adobe\Acrobat Reader DC\ | 2022-04-15 | 2022-05-12 14:11 |
| | AhnLab Safe Transaction | 1.5.1.1581 | C:\Program Files\AhnLab\Safe Transaction | 2020-08-05 | 2022-05-12 14:11 |
| | Amazon | 2018.519.2815.0 | C:\Program Files\WindowsApps\Amazon.com.Amazon_2018.519.2815.0_x64__343d40qqvtj1t | | 2022-05-12 14:11 |
| | AnySign4PC 1.1.3.3 | 1.1.3.3 | | | 2022-05-12 14:11 |
| | Apple 응용 프로그램 지원(32비트) | 6.4 | C:\Program Files (x86)\Common Files\Apple\Apple Application Support\ | 2018-05-09 | 2022-05-12 14:11 |
| | Apple 응용 프로그램 지원(64비트) | 6.4 | C:\Program Files\Common Files\Apple\Apple Application Support\ | 2018-05-09 | 2022-05-12 14:11 |
| | AsyncTextService | 10.0.19041.1023 | C:\Windows\SystemApps\Microsoft.AsyncTextService_8wekyb3d8bbwe | | 2022-05-12 14:11 |
| | Autodesk SketchBook | 5.1.0.0 | C:\Program Files\WindowsApps\89006A2E.AutodeskSketchBook_5.1.0.0_x64__tf1gferkr813w | | 2022-05-12 14:11 |
| | Beauty Camera | 2.0 | | 2018-10-16 | 2022-05-12 14:11 |
| | Bonjour | 3.1.0.1 | C:\Program Files (x86)\Bonjour\ | 2018-05-09 | 2022-05-12 14:11 |
| | BrainPOP ESL | 1.3.9.0 | C:\Program Files\WindowsApps\BrainPOPLLC.BrainPOPESL_1.3.9.0_x64__w5m80jq9t906m | | 2022-05-12 14:11 |
| | Canon Office Printer Utility | 12.7.0.0 | C:\Program Files\WindowsApps\34791E63.CanonOfficePrinterUtility_12.7.0.0_x64__6e5tt8cgb93ep | | 2022-05-12 14:11 |
| | CapturePicker | 10.0.19041.1023 | C:\Windows\SystemApps\Microsoft.Windows.CapturePicker_cw5n1h2txyewy | | 2022-05-12 14:11 |
| | Chrome | 101.0.4951.64 | C:\Program Files (x86)\Google\Chrome\Application | 2022-05-12 | 2022-05-12 14:11 |
| | ColorEngine | 4.4 | | 2018-10-16 | 2022-05-12 14:11 |
| | Consulting Mode Touchpad Driver | 20.0.0.24 | | | 2022-05-12 14:11 |
| | CoreAAC Audio Decoder (remove only) | | | | 2022-05-12 14:11 |
| | Cortana | 4.2203.4603.0 | C:\Program Files\WindowsApps\Microsoft.549981C3F5F10_4.2203.4603.0_x64__8wekyb3d8bbwe | | 2022-05-12 14:11 |

| 순 서 | 설 명 | |
|---|---|---|
| 1 | 설치된 단말의 소프트웨어 정보 수집<br>- 백신 정보: 설치된 백신명/ 패턴 버전/ 패턴 날짜/ 실시간감시설정/ 최근검사<br>- 소프트웨어: 소프트웨어명/ 버전/ 설치경로/ 설치일자 등<br>- 필수소프트웨어 강제 배포, 비인가 프로그램 삭제, 프로세스 킬 등 | 사전 배포를 통해 NAC Agent가 설치되면 백신/ 일반 소프트웨어 정보 등을 수집할 수 있습니다. 차후 필수 소프트웨어 배포, 프로세스 킬 등의 정책운영을 위한 정보가 됩니다. |

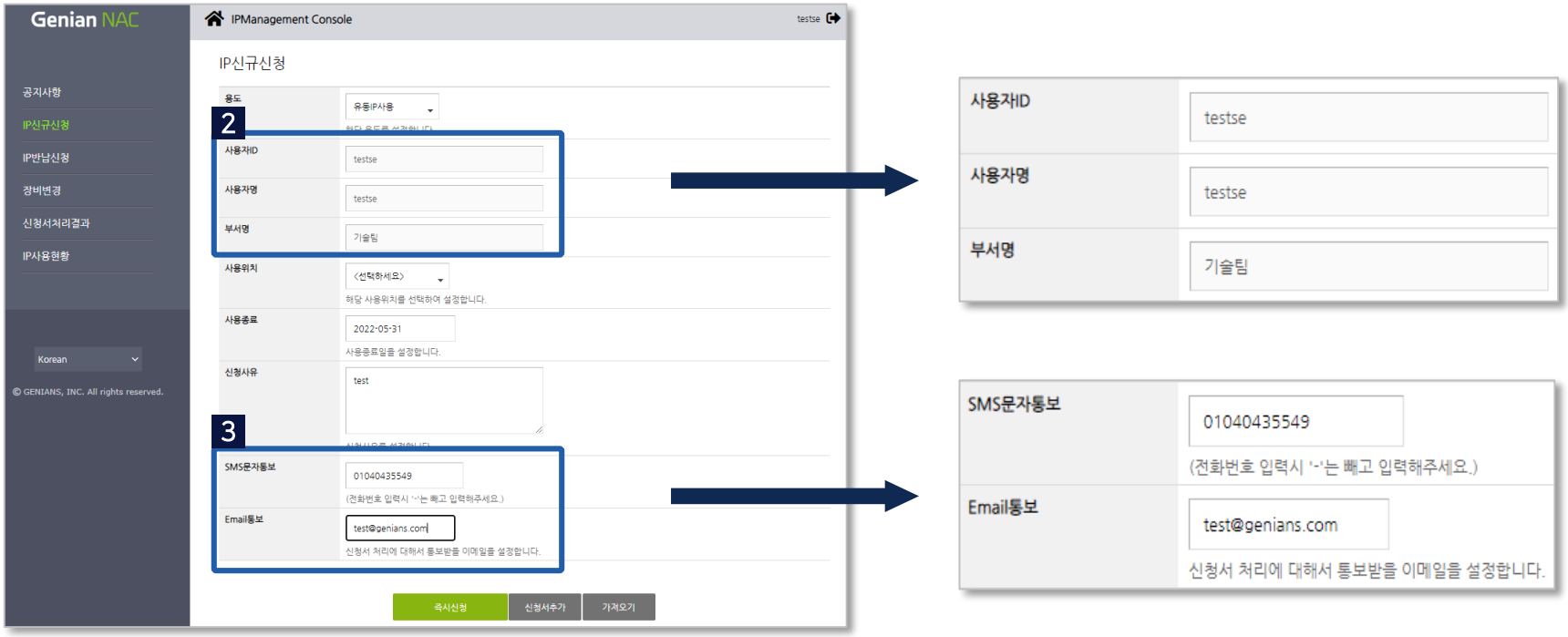
# 사용자 영역 (IP 관리시스템)

## Phase: 가시성 확보 → 비인가단말제어 → 인증 → 무결성검사


| 순 서 | 설 명 | |
|---|---|---|
| 1 | 승인되지 않은 단말이 내부망에 연결 | 승인되지 않은 비인가 단말을 연결하면 IP사용신청 페이지(전통적인 IP관리)로 전환됩니다. |
| 2 | 네트워크 사용이 차단되고 웹브라우저 사용시 “비인가” 상태 확인 | |
| 3 | IP”사용신청” 진행 (IPM) | |

# 사용자 영역 (IP 관리시스템)

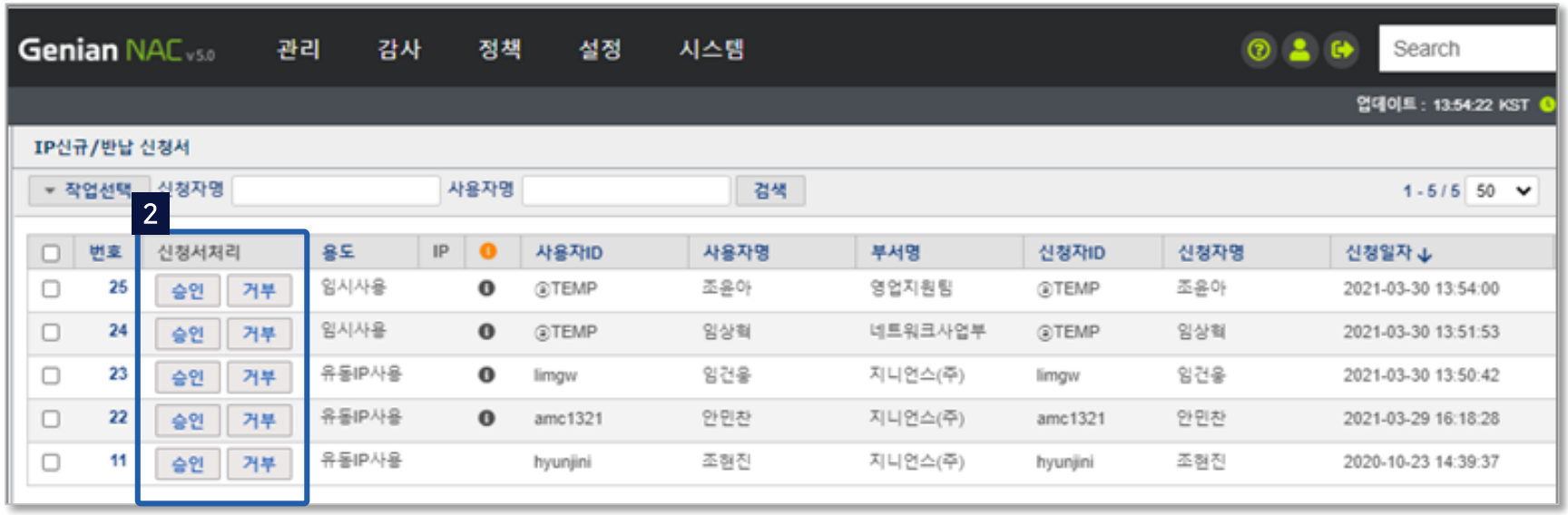
## Phase: 가시성 확보 → 비인가단말제어 → 인증 → 무결성검사




| 순 서 | 설 명 | |
|---|---|---|
| 1 | 신청자의 계정으로 IP"사용신청" 시스템 로그인 | 신청자는 웹기반으로 신규 단말에 대한 사용신청을 진행할 수 있습니다.<br>사내 인사DB를 연동하여 신청자의 편의성을 확보할 수 있습니다. |
| 2 | 신청자 정보 확인 및 작성<br>- 인사DB 연동을 통해 사용자 지정 시 사용자명/ 부서 등 자동표시 | |
| 3 | IP사용 신청 결과를 SMS/Email로 수신할 수 있도록 통보 방법 작성 | |

# 사용자 영역 (IP 관리시스템)

## Phase: 가시성 확보 → 비인가단말제어 → 인증 → 무결성검사




| 순 서 | 설 명 | |
|---|---|---|
| 1 | IP신청이 발생시 관리자는 SMS(혹은 E-Mail)로 신청 발생을 인지 | 사용자가 IP사용 신청을 하면 관리자는 NAC 관리 콘솔에 접속하여 승인/ 거부 과정을 진행합니다.<br>신청서가 처리되면 사용자(신청자)에게 알림 메시지가 전송됩니다. |
| 2 | 관리 WEBUI 에서 IP신청서를 승인/거부 | |
| 3 | 추가 기능<br>- 주요 장비의 충돌보호, 사용자 PC의 변경 금지 설정 등 | |

# 사용자 영역

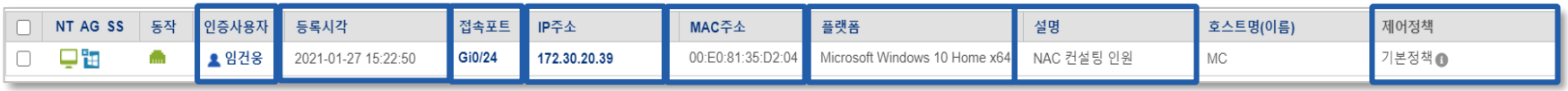
## Phase: 가시성 확보 → 비인가단말제어 → 인증 → 무결성검사


| 순 서 | 설 명 | |
|---|---|---|
| 1 | IP사용 승인 후 NAC 사용자 인증: IP실명제 | 기기에 대한 승인 이후 사용자에 대한 인증을 진행합니다. 내부직원은 연동된 인사DB의 아이디 기반으로 인증을 진행하고 외부 사용자는 “사용자 등록 " 을 통해 계정신청을 요청할 수 있습니다. |
| 2 | 인증된 사용자 정보는 연동된 문서보안, PC보안 에이전트 등에 인증정보를 전송하여 불필요한 인증과정 제거 | |
| 3 | 추가기능<br>- 외부직원, 프로젝트팀 등 인사DB에 없는 사용자는 “사용자등록” 진행<br>- 사용자별 인증 가능한 IP/ MAC, 개수 지정 가능<br>- 아이디/ 비밀번호 찾기(초기화) 기능: SMS, E-Mail<br>- 인증주기: IP/MAC 변경시, 시간, 부팅시 재인증 등 | |

# 관리자 영역

## Phase: 가시성 확보 → 비인가단말제어 → 인증 → 무결성검사

1 누가? 2 언제? 3 어디서? 4 어떤 IP/MAC으로? 5 어떤 장비로? 6 어떤 목적으로? 7 어떤 정책을?




| | GUI Column | Sample - GUI Value |
|---|---|---|
| 1. 누가? | 인증 사용자 | 임건웅 |
| 2. 언제? | 최근 동작, 최초 사용 시각 | 2021년 01월 27일 15시 22분 50초 |
| 3. 어디서? | 스위치, 포트 | 내부 Switch Gi0/24 번 포트 |
| 4. 어떤 IP로? | IP주소 / MAC주소 | 172.30.20.39 / 00:E0:81:35:D2:04 |
| 5. 어떤 장비로? | 플랫폼 | Windows 10 Home x64 를 이용하는 단말 |
| 6. 어떤 목적을? | 설명 [관리자가 설정하는 설명 글] | 외부에서 컨설팅 목적으로 들어온 인원 |
| 7. 어떤 정책을? | 네트워크 정책 | (Role Base Access Control) 협력업체 **[IP별 / 서비스별 / 시간별 정책설정]** |

IP 관리 시스템에서 제공되는 부분

| 순 서 | 설 명 | |
|---|---|---|
| 1 | IP 실명제 완료 | 사용자 인증을 통해 “IP실명제”가 완료되었고 확보된 사용자기반의 가시성을 통해 사용자/ 부서별 정책에 활용할 수 있습니다. |
| 2 | 네트워크에 연결된 단말별 사용자 정보 수집 완료 | |

# 사용자 영역

## Phase: 가시성 확보 → 비인가단말제어 → 인증 → 무결성검사


| 순 서 | 설 명 | |
|---|---|---|
| 1 | 필수 소프트웨어 설치 강제화 | NAC Agent가 설치되면 사용자 단말의 가시성을 확보하고 보안 무결성 항목에 대한 강제화를 수행할 수 있습니다.<br><br>※ Windows에서 연동 가능한 백신목록<br>V3, ViRobot, ALYac (알약 연동 모듈) |
| 2 | 불법 소프트웨어 설치 시 차단, 불법 프로세스 차단 | |
| 3 | OS 보안 강제화<br>- 공유폴더/ 화면보호기/ 윈도우 방화벽/ 호스트명 변경(인사DB 활용)<br>- 사용자계정 정보: 비밀번호 규칙(변경주기)/ 계정타입(관리자, 사용자)에 따른 접근 제어 | |
| 4 | 보안/ 중요/ 업데이트/ 업데이트 롤업 등의 패치 | |

# 04.

# 회사소개

# 지니언스㈜

## NAC 기술 기반 보안 플랫폼 기업, 지니언스


| 회 사 명 | 지니언스(주) |
|---|---|
| 대표이사 | 이 동 범 |
| 설 립 일 | 2005년 01월 06일 |
| 자 본 금 | 20억 |
| 주요사업 | 네트워크 보안 솔루션 개발/판매,<br>보안감사(audit) 솔루션 개발/판매 |
| 임직원수 | 189명 (2024년 04월 기준) |
| 협 력 사 | 론스텍(총판), 대신정보통신(총판) 등 약 100개사 |
| 주 소 | 경기도 안양시 동안구 벌말로 66 평촌역 하이필드<br>지식산업센터 A동 12층 |
| 홈페이지 | https://www.genians.co.kr |

# 지니언스㈜

## 지니언스는 탄탄한 기술력을 바탕으로 보안의 영역을 넓히며 성장해왔습니다.

### 원천기술 확보

**2005**
01. 지니네트웍스㈜ 설립

**2006**
03. 네트워크 접근제어 솔루션 Genian NAC v1.5 출시

### 국내 NAC 시장 선도

**2008**
10. 기술혁신형 중소기업(INNO-BIZ) 선정
08. 지식경제부 우수보안기술 업체 선정

**2012**
07. 유무선 네트워크 접근제어 Genian NAC Suite v4.0 출시
06. 안양 평촌 사옥 이전

**2013**
10. Genian 내PC지키미 v3.0 GS 인증 획득

### 글로벌 사업 확대

**2016**
02. 미국 RSA 2016 참가
01. 미국법인 GENIANS, INC. 설립

**2017**
08. 코스닥 상장
03. 지니언스㈜ 사명 변경
02. EDR 솔루션 'Genian Insights E' 출시

### EDR 시장 진출

**2018**
02. IoT·클라우드 지원 네트워크 접근제어 솔루션 Genian NAC v5.0 출시
01. 머신러닝 엔진 탑재 EDR 'Genian Insights E' 출시

**2019**
12. EDR 사업 부문, 공공·금융·제조 대형 레퍼런스 확보
11. 미주·유럽·중동에 클라우드 기반 차세대 NAC 공급
09. 전 세계 33개국 34개 현지 파트너 확보

### 글로벌 보안 플랫폼으로 확장

**2020**
12. 지니언스 미국법인, 실리콘밸리로 이전
09. 가트너 '차세대 NAC' 대표기업 선정
05. Genian NAC Frost & Sullivan 글로벌 마켓 리프트 등재
01. EDR 솔루션 'Genian Insights E v2.0' 출시

**2021**
12. ZDR/NDR 전문 기업 엑사비스와 XDR 사업 투자 협정
10. 중기·스타트업 대상 혁신중소기업부문 중소벤처기업부 장관상(대상)
06. 가트너 NAC 마켓가이드 대표 기업 선정

**2022**
02. 가트너 선정 '글로벌 톱5 NAC 업체' 진입

**2023**
06. KISA / ZT 실증 과제 컨소시엄
07. NSR / ZTNA 보안모델 실증

# 주요 고객사

## 기업


## 금융


## 공공기관

# Together.
# More Secure.