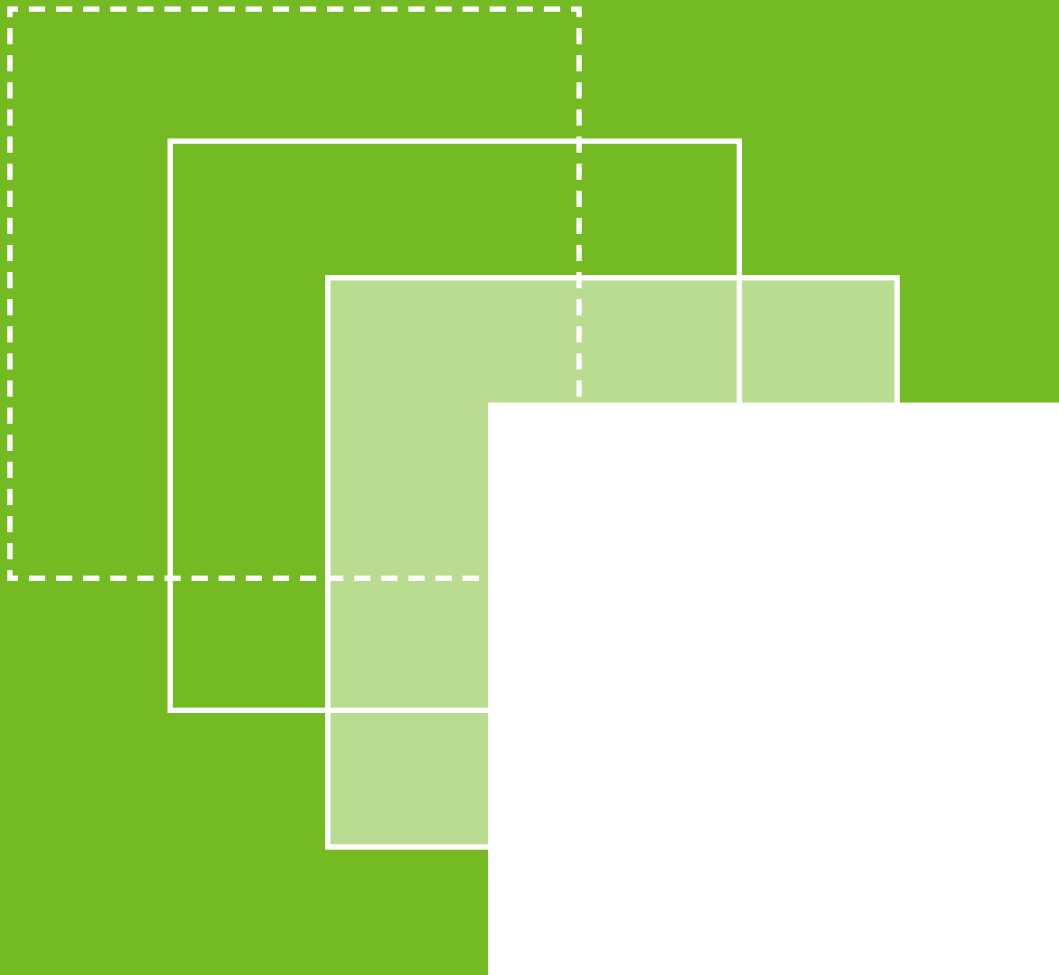


네트워크 접근 제어 솔루션

# Genian NAC

v 5.X

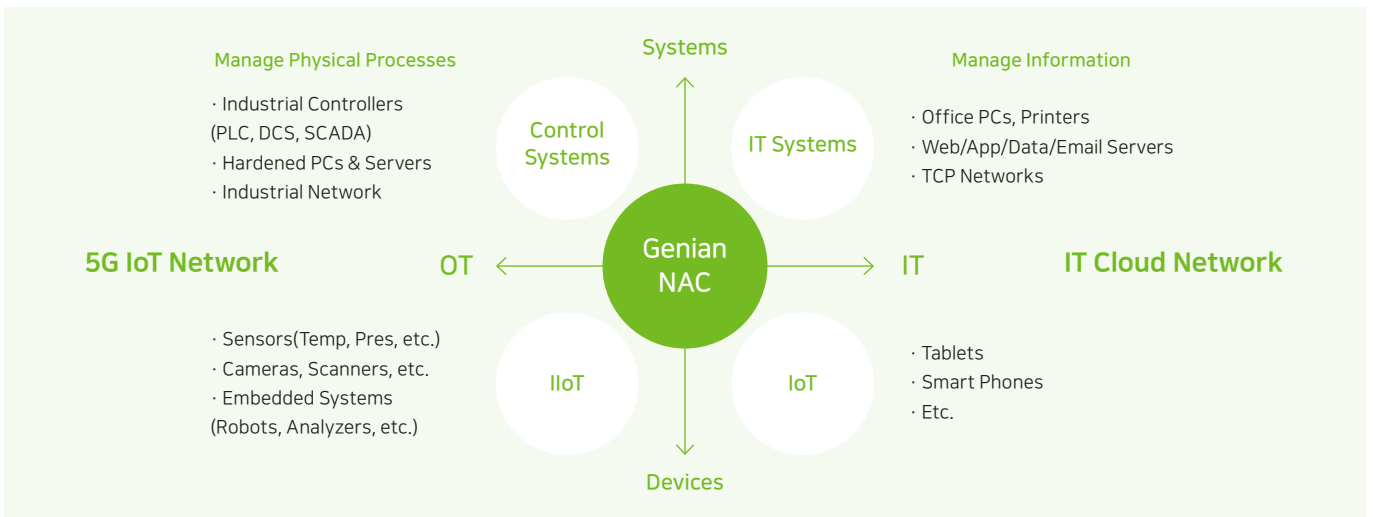


# Genian NAC

## Overview

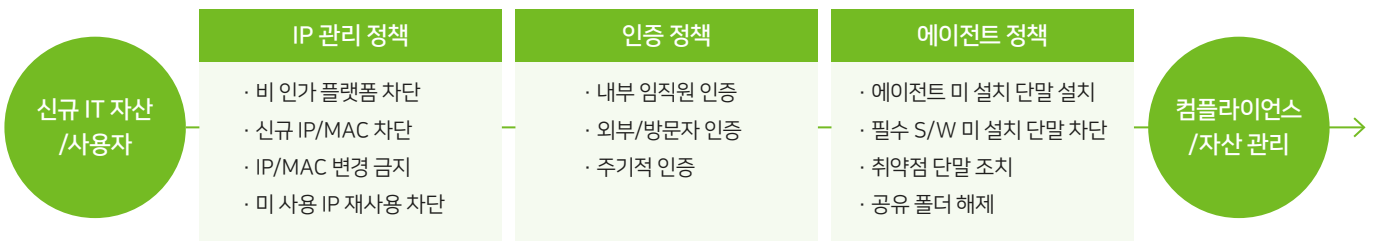
IoT 시대 개인이 사용하는 IT 기기는 빠르게 늘어나고 있습니다. 업무에 사용하는 스마트폰, 태블릿 등은 물론 개인이 사용하는 웨어러블 기기까지 기업의 네트워크에 연결된 디바이스가 늘어날수록, 보안 관리자의 고민도 함께 늘어납니다. 네트워크에 어떤 종류의 단말이 존재하는지, 현재 어떤 상태인지, 어떤 활동을 하고 있는지에 대한 가시성(Visibility) 확보는 내부 보안을 위한 첫걸음입니다. '지니안 NAC(Genian NAC)'는 내부 정보 보호 체계를 수립하여 내부 자산과 사용자를 보호하고 기업 자원을 안전하게 사용할 수 있도록 지원하는 유무선 네트워크 접근제어(NAC: Network Access Control) 솔루션입니다.

강력한 인증을 통해 자산과 사용자를 식별하고, 네트워크 접근에 대한 권한을 차등 부여하며, 특정 단말 및 IP/서브넷/VLAN 등 사용자 접속 권한을 제어합니다. 사용자의 단말 보안 상태를 점검 및 조치하여 네트워크를 청정하게 유지하며 BYOD 환경에서 유무선을 아우르는 내부 보안 관리 체계를 완성할 수 있습니다.



## 도입 효과

Genian NAC를 통해 내부에 연결되는 모든 IT 자산에 대한 가시성을 확보할 수 있습니다. 이는 자산 관리의 효율을 높여줄 뿐 만 아니라 보안 프로세스와 연계하여 조직 전체의 보안 수준을 고도화합니다. 단계별 보안 정책의 적용 및 강제화, 점검을 통해 강력하고 누수 없는 보안 관리 체계를 구축하고 운영할 뿐 아니라 타 솔루션과의 연동을 통하여 내부 보안을 위한 통합 인프라로 활용할 수 있습니다.



- SW 통제 필수 SW 설치 현황 파악 및 미 설치 단말의 차단/설치 유도
- 인증 강화 인증 시스템 연동을 통한 미 인증 사용자 제어 및 IP 실명제
- 통합 관리 전사 단말기 현황 파악 및 통합 관리 시스템 구축
- IP 관리 네트워크에 연결된 모든 장치에 대한 IP/MAC 관리 시스템 구축
- 플랫폼 분류 Agent 설치 없이 OS 종류, 모델명, 버전, 제조사 등의 정보 제공
- 네트워크 통제 보안 위협 단말 차단 및 사용자 접근통제를 통한 안전한 네트워크 구현

# Product Function

## 내부 보안(관리)을 위한 다양한 핵심 기능 제공



### 네트워크 접근 제어

- 속성 기반 접근통제(ABAC: Attribute Based Access Control)
- 표준 802.1X 지원(RADIUS) 및 Dynamic Vlan제공
- DHCP 서버 내장 및 할당 제어
- ARP 기반 Layer 2 지원
- 포트 미러링 및 방화벽/스위치 통합 기반 제어



### 무선 네트워크 접근 제어

- SSID별 접속 단말 현황 파악
- 사용자 기반 AP 위치 정보 제공
- 불법(Rogue) AP 탐지 및 유선/에이전트를 통한 전방위 통제
- SoftAP/Adhoc/Hidden SSID 등 다양한 무선랜 정보 제공
- 무선 접속 매니저(EAP-GTC) 제공 및 802.1X 지원



### 사용자 인증관리

- 자체 포털(CWP) 사용자 인증 지원
- 기존 인사 DB 및 타 솔루션 인증 연동
- AD(Active Directory) 인증 연동(SSO)
- 802.1X 기반 RADIUS 제공 및 Dynamic Vlan지원
- LDAP, SMTP, POP3, IMAP 등 외부 인증 연동
- SAML(Google G Suite, Okta) 인증 연동
- 지문인식 및 OTP(Google OTP 등) 연동



### IP 관리

- 독립 솔루션 수준의 IP 관리 기능 제공
- IP/MAC 제어(사용시간, 사전예약 등)
- IP/MAC 충돌보호/변경금지
- IP/MAC 스푸핑(Spoofing) 감지
- DHCP 제공 및 IP신청/승인 등 업무절차 지원
- 인사 DB 연동을 통한 IP실명제 및 이력관리
- 감사 대비 자료 제출용 이력 정보 추출 기능 제공



### 데스크톱 관리

- 모든 데스크톱의 자동 탐지 및 식별
- 내부 자산정보 변경 관리
- 하드웨어 및 운영체제 환경 설정(DNS 설정 등)
- '언제, 어디서, 누가, 무엇을'의 현황 관리
- 실시간 상세(H/W, S/W, 패치, WMI 등) 정보 수집



### 단말 탐지/식별 및 관리

- DPI(Device Platform Intelligence) 기반 단말 상세 정보 제공 (단말 종류, 운영체제 정보, EOL/EOS, CVE 등)
- Switch Port 정보 수집
- 500여 가지 조건에 따른 단말 자동 분류
- 단말 변경 사항 추적/감사 등



### 연동 관리

- User Directory 연동(RDBMS, LDAP)
- Syslog/REST API/Webhook/SNMP Trap 등 지원
- ORACLE/MYSQL/DB2/Tibero/Altibase/CSV 등 연동
- V3 등 백신 및 Palo Alto Networks, Fireeye 제품과 연동



### 패치 및 소프트웨어 관리

- WSUS 기반 MS Windows 및 Office 패치 관리
- 패치 적용 시점 및 백그라운드 설치
- 패치 설치 대상 및 승인 여부 관리
- 독립 배포 서버 구축(폐쇄망 및 오프라인 패치 지원)
- 관리자 지정 소프트웨어 배포 및 설치(백신 등)
- 규정 위반 소프트웨어에 대한 원격/강제 삭제 등
- 일반파일 배포 및 설치 지원



### 장치 관리

- USB, CD-RW 등 장치(Device) 사용 통제
- 매체(Media) 관리 솔루션 대비 높은 안정성



### 위협 및 취약점 관리

- 주요 백신의 버전, 업데이트 등 정보 관리
- V3, 알약 등 4대 백신 연동(강제 검사, 업데이트 등 지원)
- 단말 취약점(CVE: Common Vulnerability&Exposure) 확인



### 기타/일반 관리

- 100가지 이상 위젯(Widget) 기반의 대시보드 지원
- 기본 리포트 및 고객 맞춤형 리포트 제공
- 관리용 Mobile App(Android/iOS) 제공
- 이중화 구성 지원(Policy Server/Network Sensor)
- 다국어 지원(한국어/영어/일어/중어)

# Product Function

## 보안 강화

보안 정책 위반 행위에 대하여 다양한 대응 방법을 제공합니다. 사용자 권고 및 대응적 조치와 예방적 조치의 동시 수행으로 보안 관리의 효율을 극대화할 수 있습니다.

알림(Alarm)	차단(Block)	교정(Remediation)
<ul style="list-style-type: none"> <li>· 사용자에게 알림 (차단 웹, 에이전트 팝업, 인스턴스 메시지)</li> <li>· 관리자에게 알림 (특정 이벤트 발생 시 SMS, E-mail 발송)</li> <li>· 특정 로그 외부 전송 (타 보안 솔루션으로 로그 전송하여 모니터링)</li> </ul>	<ul style="list-style-type: none"> <li>· 조건에 따른 네트워크 차단 (신규 IP/MAC, 미 인증, 보안 설정 위반 등)</li> <li>· 특정 프로세스 중지 (관리자가 지정한 프로세스)</li> <li>· USB 장치 차단 (USB 저장 장치 등 강제 Off)</li> </ul>	<ul style="list-style-type: none"> <li>· 필수 SW 설치 유도 (백신, DRM, DLP 등 보안 솔루션 강제 설치)</li> <li>· 불법 SW 삭제 (허용되지 않은 특정 SW 강제 삭제)</li> <li>· 보안 설정 강제화 (패스워드 설정, 화면보호기 등)</li> </ul>






## 에이전트(Agent) 설치

에이전트 설치 유/무에 따라 단말 내부의 상세 정보 수집 및 제어의 범위가 다릅니다. 에이전트 설치는 조직의 보안 정책 및 관리 수준에 따라 선택적 적용이 가능합니다.

### Agent-less

구분	세부 정보
플랫폼 분류	OS(Windows, Linux, Unix, iOS, Android 등), 네트워크 장비, 프린터, 제조사 등
접근제어	IP, MAC, PORT, Protocol 별 접근 제어 플랫폼 별 접근 제어(OS 및 장치 별)
	시간/요일/기간 접근 제어 사용자 별 접근 제어 (인증/미 인증, ID, 부서, 직급 등)
네트워크 정보	IP 관리(IP/MAC 고정, 변경 금지, 충돌 보호, 사용시간 등)
	사용자 PC가 연결된 스위치 및 포트 정보 호스트명, 도메인명
	PC 동작 유무 판단, PC 열린 포트 정보

### Agent

OS	구분	세부 정보
	Windows 패치	Windows patch(PMS) 기능 제공
	세션 제어	TCP 세션 정보 수집 및 임계치 초과 시 차단
	포트 정보	열린 포트, 포트 사용 프로세스, 서비스 정보
	백신 연동	백신(V3, 바이로봇, 알약) 업데이트 및 바이러스 탐지에 대한 네트워크 제어
	소프트웨어 탐지	필수 S/W, 불법 S/W 탐지 및 제어
	위 변조 탐지	IP, MAC clone 탐지/차단
	보안 기능	비밀번호 유효성 검사, 윈도우 보안 설정, 자동 실행 제어, 파일 배포, 화면보호기 제어, IE 보안 설정 제어, 윈도우 방화벽 제어, 계정 취약성 검사, 공유 폴더 제어
	macOS 업데이트	macOS 자동 업데이트 기능 제공
	보안 기능	화면보호기 제어, 무선랜 제어, 에이전트 인증창, 호스트명 변경
	Linux 업데이트	Linux OS 자동 업데이트 기능 제공 (Ubuntu, Gooroom, TmaxGooroom, HamoniKR)
	장치 제어	USB, NIC, Bluetooth, Wifi, Tethering, PC전원 제어
	프로세스 제어	특정 프로세스 강제 종료
	메시지 전송	사용자에게 메시지 전송(공지 및 알림 팝업)
	AP 탐지	무선 AP 탐지 및 접속 제어
	시스템 정보	PC OS 및 H/W 정보(CPU, MEM, DISK, NIC 등), S/W 정보, 호스트명 수집 및 제어

\* Agent 없는 환경에서도 다양한 방식으로 접근 제어

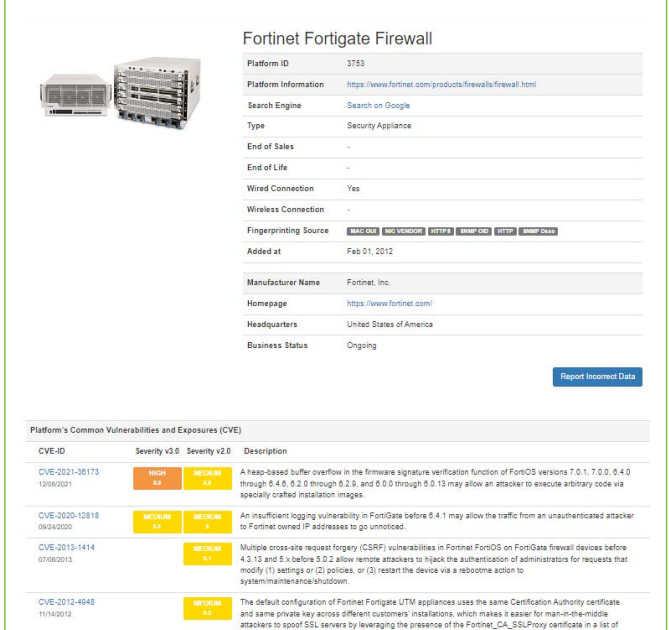
# Key Features

## 가시성 확보

DPI는 네트워크에 연결된 IT 자산(단말 등) 및 OT 자산을 실시간으로 탐지하여 식별하고 상세하게 분류합니다. 단말의 일반 정보는 물론 확장 정보와 취약점 정보까지 제공하여 생명주기 관리까지 업무 영역을 확대할 수 있습니다. 일반 IT 환경뿐 아니라 공장, 설비 등의 OT 환경에서도 적용 가능합니다.

등록상태자트	IP주소 ↑	MAC주소	정책	제어정책	호스트명(이름)	NIC벤더	플랫폼
	172.29.254.100	04:D5:90:8F:9F:83		기본정책	(Fortigate#1)	Fortinet, Inc.	Fortinet Fortigate Firewall
	172.29.254.110	04:D5:90:9B:2A:E0		기본정책	(Fortigate#2)	Fortinet, Inc.	Fortinet Fortigate Firewall

구분	세부 정보
단말 식별 정보 (Device Identity)	<ul style="list-style-type: none"> <li>· 단말 제조사, 이름, 모델번호</li> <li>· 단말 사진</li> <li>· 네트워크 연결 방식(Wired/Wireless)</li> <li>· 단말 상세 정보 URL</li> </ul>
단말 확장 정보 (Device Context)	<ul style="list-style-type: none"> <li>· 제조사 명칭</li> <li>· 제조사 홈페이지 URL</li> <li>· 본사의 위치와 현재 사업 진행 여부</li> <li>· 제품 판매 종료(End of Sales) 여부</li> <li>· 제품 지원 종료(End of Support) 여부</li> <li>· 검색엔진 연결 URL</li> </ul>
단말 위협 정보 (Device Risk)	<ul style="list-style-type: none"> <li>· 단말에 알려진 CVE 정보 (CVE No./Severity/Description 등)</li> <li>· 제조사에 알려진 CVE 정보 (CVE No./Severity/Description 등)</li> </ul>



**Fortinet Fortigate Firewall**

Platform ID: 3783

Platform Information: <https://www.fortinet.com/products/firewall/firewall.html>

Search Engine: Search on Google

Type: Security Appliance

End of Sales: -

End of Life: -

Wired Connection: -

Wireless Connection: -

Fingerprinting Source:  MAC OS  WINDOWS  HTTP  SNMPv2  HTTP  SNMPv3

Added at: Feb 01, 2012

Manufacturer Name: Fortinet, Inc.

Homepage: <https://www.fortinet.com/>

Headquarters: United States of America

Business Status: Ongoing

[Report Incoming Data](#)

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

CVE-ID	Severity v3.0	Severity v2.0	Description
CVE-2021-38173 12/08/2021	HIGH	MEDIUM	A heap-based buffer overflow in the firmware signature verification function of FortiOS versions 7.0.1, 7.0.0, 6.4.0 through 5.4.6, 6.2.0 through 6.2.0, and 6.0.0 through 6.0.13 may allow an attacker to execute arbitrary code via specially crafted installation images.
CVE-2020-12818 09/24/2020	MEDIUM	MEDIUM	An insufficient logging vulnerability in FortiGate before 6.4.1 may allow the traffic from an unauthorized attacker to Fortinet owned IP addresses to go unnoticed.
CVE-2013-1414 07/09/2013	MEDIUM	SP	Multiple cross-site request forgery (CSRF) vulnerabilities in Fortinet FortiOS on FortiGate firewall devices before 4.0.10 and 5.x before 5.0.2 allow remote attackers to hijack the authentication of administrators for requests that modify (1) settings or (2) policies, or (3) restart the device via a rebornme action to system/maintenance/shutdown.
CVE-2012-4648 11/14/2012	MEDIUM	SP	The default configuration of Fortinet Fortigate UTM appliances uses the same Certification Authority certificate and same private key across different customers' installations, which makes it easier for man-in-the-middle attackers to spoof SSL servers by leveraging the presence of the Fortinet_CA_SSLProxy certificate in a list of trusted root certification authorities.

DPI가 제공하는 단말 관련 정보

DPI를 이용한 'Fortinet' 단말 확인

## 단말 취약점(CVE) 관리

네트워크에 존재하는 단말의 취약점(CVE) 정보를 확인할 수 있습니다. 제조사 및 플랫폼 별 신규 취약점이 발표되는 경우 해당 단말을 빠르게 찾아 조치할 수 있습니다.

**CVE 심각도별 카운트**

3 CRITICAL    19 HIGH    24 MEDIUM    1 LOW

**CVE 플랫폼별 현황**

CVE-ID	노드수	플랫폼수 ↓	Published	LastModified	Severity
CVE-2020-11899	1	404	2020-06-17	2022-07-11	MEDIUM
CVE-2022-30226	38	39	2022-07-13	2022-07-21	HIGH
CVE-2022-30225	38	39	2022-07-13	2022-07-21	HIGH
CVE-2022-30224	38	39	2022-07-13	2022-07-21	HIGH
CVE-2022-30202	38	39	2022-07-13	2022-07-21	HIGH

[See More](#)

**최근 CVE 현황**

CVE-ID	노드수	Published	LastModified ↓	Severity
CVE-2021-0121	38	2021-11-18	2022-08-02	HIGH
CVE-2021-29907	29	2021-09-01	2022-08-02	HIGH
CVE-2008-2371	2	2008-07-08	2022-08-02	HIGH
CVE-2022-22390	29	2022-06-25	2022-07-30	HIGH
CVE-2019-5827	2	2019-06-28	2022-07-30	HIGH

[See More](#)

172.29.20.11 E0:D5:9E:57:C4:C9  
DESKTOP-AMWAS5M Microsoft Windows

노드정보    장비정보    네트워크정보    정책    정책현황    이력관리

플랫폼: Microsoft Windows

확인된 플랫폼:  지정     오직발표

노드타입:  지정     지정

확인된 노드타입: 미분류

확인된 확장 노드타입:  지정     지정

OS 유형: Windows

확인된 OS 유형: 미분류

NIC 벤더: GIGA-BYTE TECHNOLOGY CO. LTD.

플랫폼상태: www.geniens.com

CVE(중, 108,92건)

CVE-ID	Published	LastModified	Description
CVE-2022-1128	2022-07-23 09:15:00	2022-07-28 04:32:00	Inappropriate implementation in Web Share API in Google Chrome on Windows prior to 100.0.4896.60 allowed an attacker on the local network segment to leak cross-origin data via a crafted HTML page.
CVE-2022-28878	2022-07-23 01:15:00	2022-07-29 00:55:00	A Denial-of-Service vulnerability was discovered in the F-Secure Agent and in certain WebSecure products while scanning fuzed APK file it is possible that can crash the scanning engine.
CVE-2022-28877	2022-07-22 01:15:00	2022-07-28 07:39:00	This vulnerability allows local user to delete arbitrary file in the system and bypassing security protection which can be abused for local privilege escalation on affected F-Secure & WMS-Secure windows endpoint products. An attacker must have code execution rights on the victim machine prior to successful exploitation.

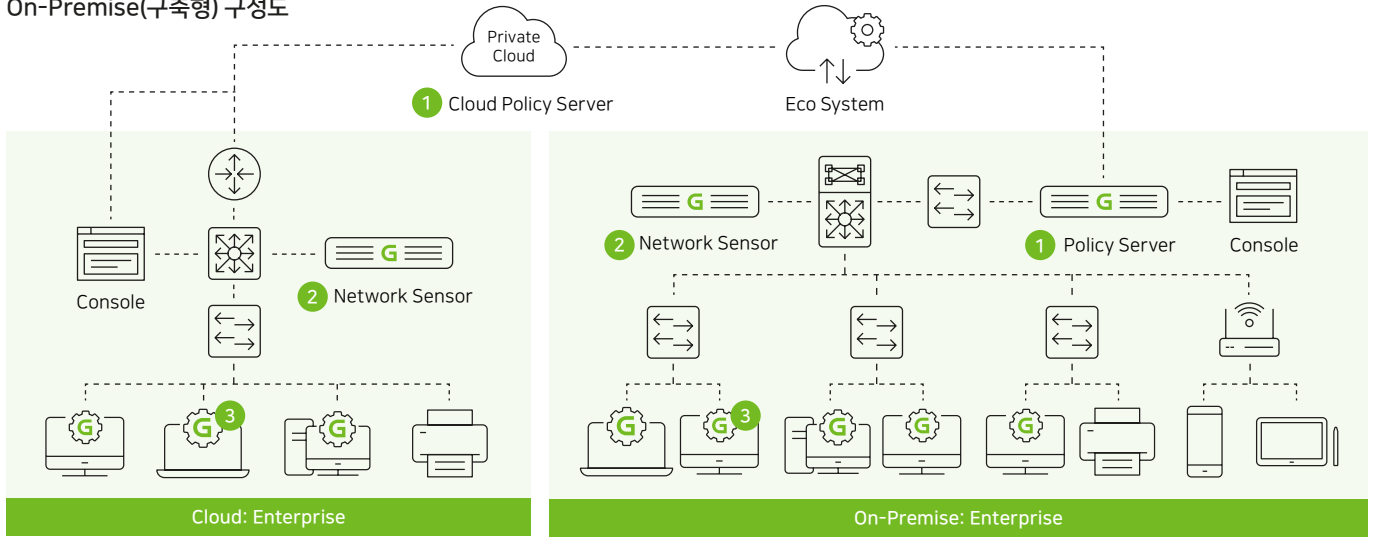
# Operating Mode

## 구성 방안

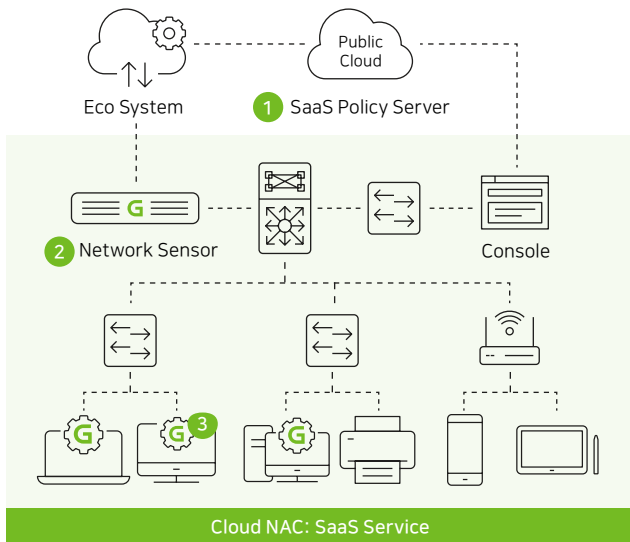
형태 및 목적에 따른 다양한 설치 및 운영 방법을 제공합니다.

On-Premise(구축형)	Cloud(SaaS)	VM(가상머신 등)
<ul style="list-style-type: none"> <li>· 기관 및 기업의 독자적인 운영 가능</li> <li>· 국내 환경에 가장 적합</li> <li>· 고객사에서 가장 선호하는 형태</li> </ul>	<ul style="list-style-type: none"> <li>· 국내 보안 솔루션 최초 클라우드 서비스</li> <li>· 보안인증(CSAP)을 받은 제품</li> </ul>	<ul style="list-style-type: none"> <li>· 서비스 사업자를 위한(MSP, MSSP, CSP, SaaS 등)</li> <li>· 다양한 플랫폼 및 운영환경 지원</li> <li>· VM, uCPE, WhiteLabeld 등 포함</li> </ul>

### On-Premise(구축형) 구성도



### Cloud(SaaS) 구성도



- 1 Policy Server&Console(정책서버&콘솔)**  
 유무선 네트워크 통합 관리, 내부 보안 강화 지원
- 2 Network Sensor(차단센서)**  
 유무선 단말에 대한 정보 수집, 강력한 통제 수행
- 3 Agent(에이전트)**  
 PC 등 에이전트 설치 단말에 자산 관리 및 장치사용 통제, 에이전트 설치에 따른 비용 부담 없음(필요에 따라 선택적 사용)

## 운영 환경

\* 상세한 내용은 Genian NAC v5.X Datasheet를 참조하십시오.

구분	Policy Server(정책서버)	Network Sensor(차단센서)	Agent(에이전트)	Console(콘솔)
사양	전용 어플라이언스(범용 OS)	전용 어플라이언스(범용 OS)	Windows XP 이상/ Mac OS X 10.9 Mavericks 이상/Linux(Debian, RedHat, openSUSE)	MS Edge 40.x 이상/ Chrome 75.x 이상/ Firefox 14.x 이상/ Safari 12.x 이상/IE 10.X 이상

# Adminstrator UI

Device Platform Intelligence / All Platforms / Microsoft Windows 10 Professional



**Microsoft Windows 10 Professional**

Platform ID: 5894

Platform Information: <https://www.microsoft.com/en-us/windowsforbusiness/default.aspx>

Search Engine: Search on Google

Type: PC

End of Sales: Planned (2025-10-14)

End of Life: Planned (2025-10-14) [more info](#)

Wired Connection: -

Wireless Connection: -

Fingerprinting Source: **HW Vendor**, **BIOS**

Added at: May 13, 2015

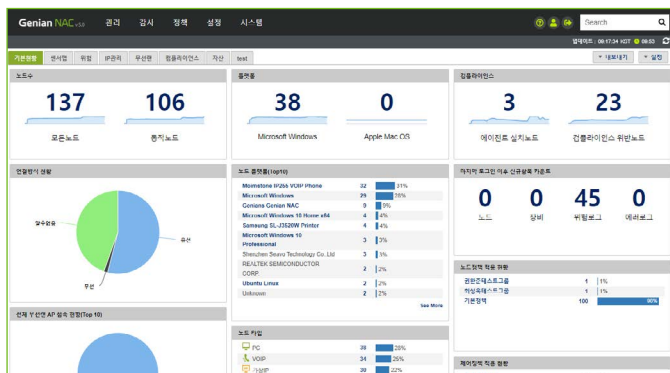
Platform's Common Vulnerabilities and Exposures (CVE)

CVE-ID	Severity v3.0	Severity v2.0	Description
CVE-2022-33644 071x20202	HIGH 7	MEDIUM 4.4	Xbox Live Save Service Elevation of Privilege Vulnerability
CVE-2022-30226 071x20202	HIGH 7.1	LOW 3.8	Windows Print Spooler Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22022, CVE-2022-22041, CVE-2022-30206.
CVE-2022-30225 071x20202	HIGH 7.4	LOW 3.8	Windows Media Player Network Sharing Service Elevation of Privilege Vulnerability
CVE-2022-30224 071x20202	HIGH 7	MEDIUM 6.8	Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-22037, CVE-2022-30202.
CVE-2022-30223 071x20202	MEDIUM 5.7	LOW 2.7	Windows Hyper-V Information Disclosure Vulnerability. This CVE ID is unique from CVE-2022-22042.

Show more

Manufacturer's Common Vulnerabilities and Exposures (CVE)

DPI(Device Platform Intelligence)



Geniun NAC... 관리 | 감사 | 정책 | 설정 | 시스템

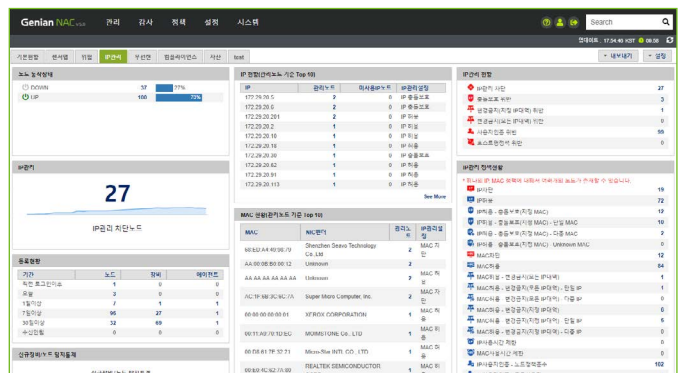
137 / 106 (모든 노드 / 활성 노드)

38 / 0 (Microsoft Windows / Apple Mac OS)

3 / 23 (에이전트 실행 노드 / 인클라인업스-위안노드)

0 / 0 / 45 / 0 (노드 / 상태 / 위험보고 / 에러보고)

0 / 0 / 45 / 0 (노드 / 상태 / 위험보고 / 에러보고)

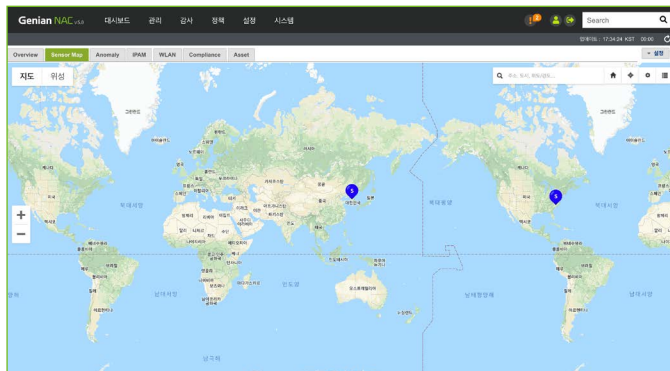


Geniun NAC... 관리 | 감사 | 정책 | 설정 | 시스템

27 (IP 관리 / 위험노드)

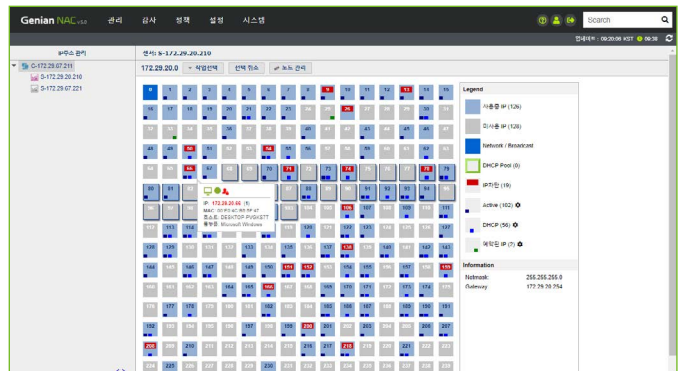
IP 관리: 172.29.20.10, 172.29.20.11, 172.29.20.12, 172.29.20.13, 172.29.20.14, 172.29.20.15, 172.29.20.16, 172.29.20.17, 172.29.20.18, 172.29.20.19, 172.29.20.20, 172.29.20.21, 172.29.20.22, 172.29.20.23, 172.29.20.24, 172.29.20.25, 172.29.20.26, 172.29.20.27, 172.29.20.28, 172.29.20.29, 172.29.20.30, 172.29.20.31, 172.29.20.32, 172.29.20.33, 172.29.20.34, 172.29.20.35, 172.29.20.36, 172.29.20.37, 172.29.20.38, 172.29.20.39, 172.29.20.40, 172.29.20.41, 172.29.20.42, 172.29.20.43, 172.29.20.44, 172.29.20.45, 172.29.20.46, 172.29.20.47, 172.29.20.48, 172.29.20.49, 172.29.20.50, 172.29.20.51, 172.29.20.52, 172.29.20.53, 172.29.20.54, 172.29.20.55, 172.29.20.56, 172.29.20.57, 172.29.20.58, 172.29.20.59, 172.29.20.60, 172.29.20.61, 172.29.20.62, 172.29.20.63, 172.29.20.64, 172.29.20.65, 172.29.20.66, 172.29.20.67, 172.29.20.68, 172.29.20.69, 172.29.20.70, 172.29.20.71, 172.29.20.72, 172.29.20.73, 172.29.20.74, 172.29.20.75, 172.29.20.76, 172.29.20.77, 172.29.20.78, 172.29.20.79, 172.29.20.80, 172.29.20.81, 172.29.20.82, 172.29.20.83, 172.29.20.84, 172.29.20.85, 172.29.20.86, 172.29.20.87, 172.29.20.88, 172.29.20.89, 172.29.20.90, 172.29.20.91, 172.29.20.92, 172.29.20.93, 172.29.20.94, 172.29.20.95, 172.29.20.96, 172.29.20.97, 172.29.20.98, 172.29.20.99, 172.29.20.100

위젯(Widget) 기반 대시보드



Geniun NAC... 관리 | 감사 | 정책 | 설정 | 시스템

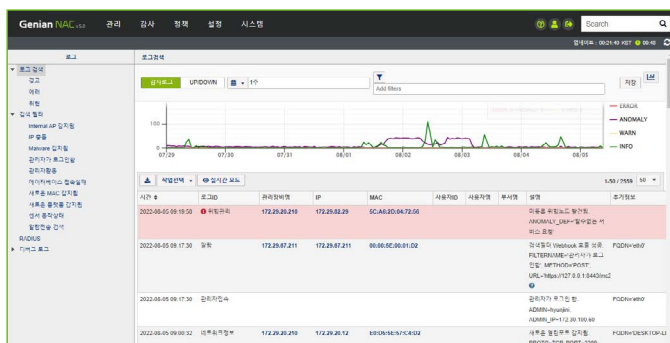
지도 위젯



Geniun NAC... 관리 | 감사 | 정책 | 설정 | 시스템

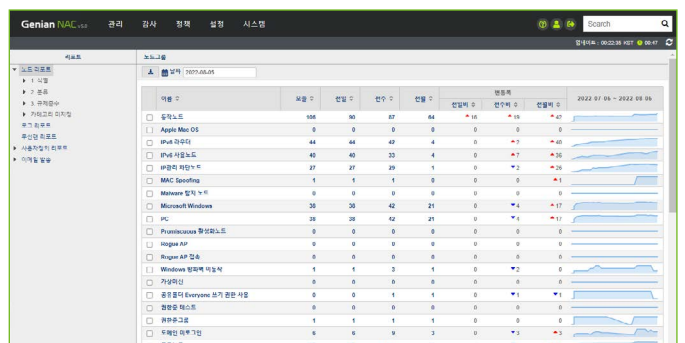
센서맵과 IP 매트릭스 뷰

센서맵과 IP 매트릭스 뷰



Geniun NAC... 관리 | 감사 | 정책 | 설정 | 시스템

감사(Audit) 및 일간 보고서



Geniun NAC... 관리 | 감사 | 정책 | 설정 | 시스템

감사(Audit) 및 일간 보고서

# 조달 디지털서비스몰

## NAC 물품식별번호

제품군	규격명	조달단가	물품식별번호
NAC 라이선스	Genian NAC Suite V5.0, NAC Node License (1~500Node)	64,900	24207921
	Genian NAC Suite V5.0, NAC Node License (501~1000Node)	44,000	24207922
	Genian NAC Suite V5.0, NAC Node License (1001Node f)	22,000	24207924
NAC 정책서버 모듈	Genian NAC Suite V5.0, NAC 정책서버모듈 (1~1000Node)	6,600,000	24207927
	Genian NAC Suite V5.0, NAC 정책서버모듈 (1001~3000Node)	13,200,000	24207929
	Genian NAC Suite V5.0, NAC 정책서버모듈 (3001~6000Node)	19,800,000	24207932
NAC 차단센서 모듈	Genian NAC Suite V5.0, NAC 차단센서모듈 (100Node ↓)	2,750,000	24207933
	Genian NAC Suite V5.0, NAC 차단센서모듈 (500Node ↓)	5,170,000	24207934
	Genian NAC Suite V5.0, NAC 차단센서모듈 (1000Node ↓)	13,530,000	24207935
	Genian NAC Suite V5.0, NAC 차단센서모듈 (2000Node ↓)	18,920,000	24207936

\* 다량납품 할인을

- 350,000,000 이상 2.5% 할인

- 500,000,000 이상 5% 할인

\* 나라장터종합쇼핑몰: <https://digitalmall.g2b.go.kr/>