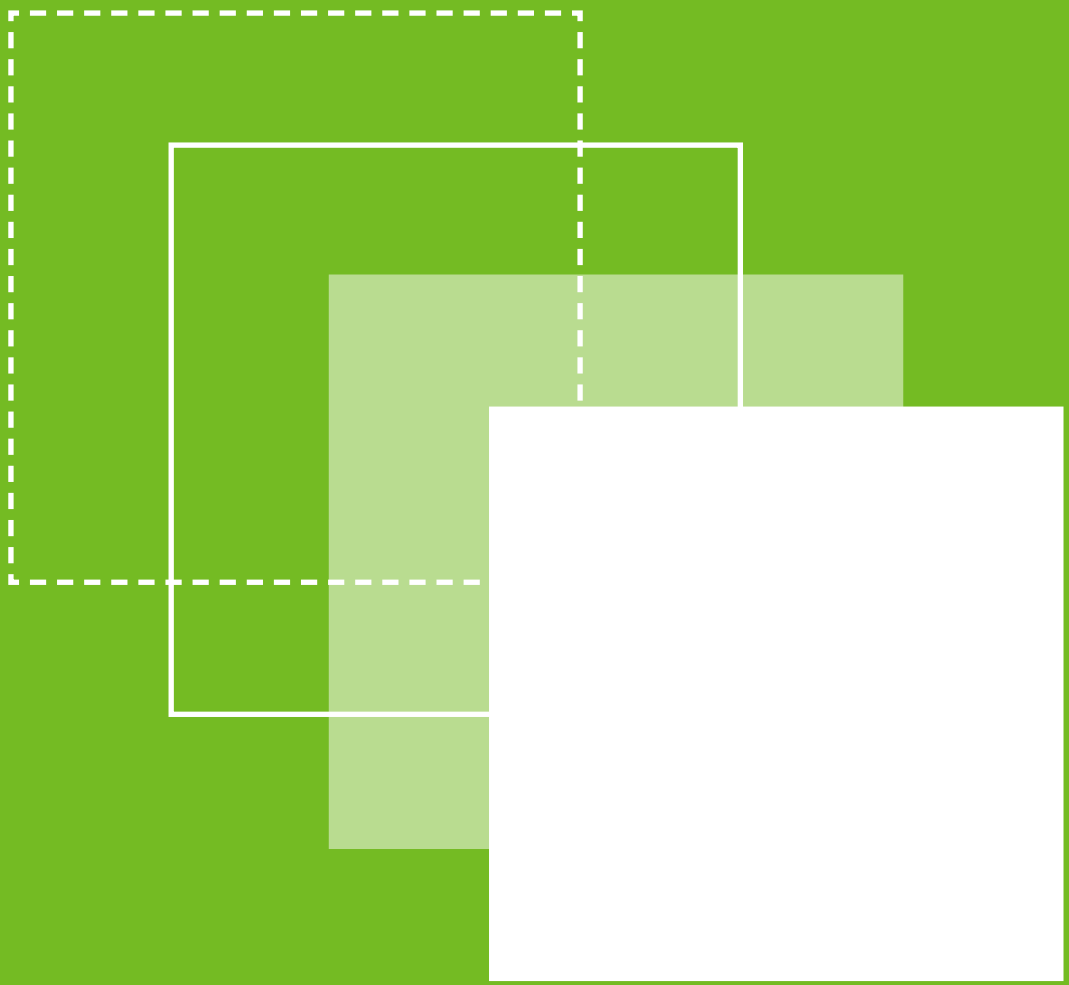
네트워크 접근 제어 솔루션

Genian NAC

v 5.X



Genians

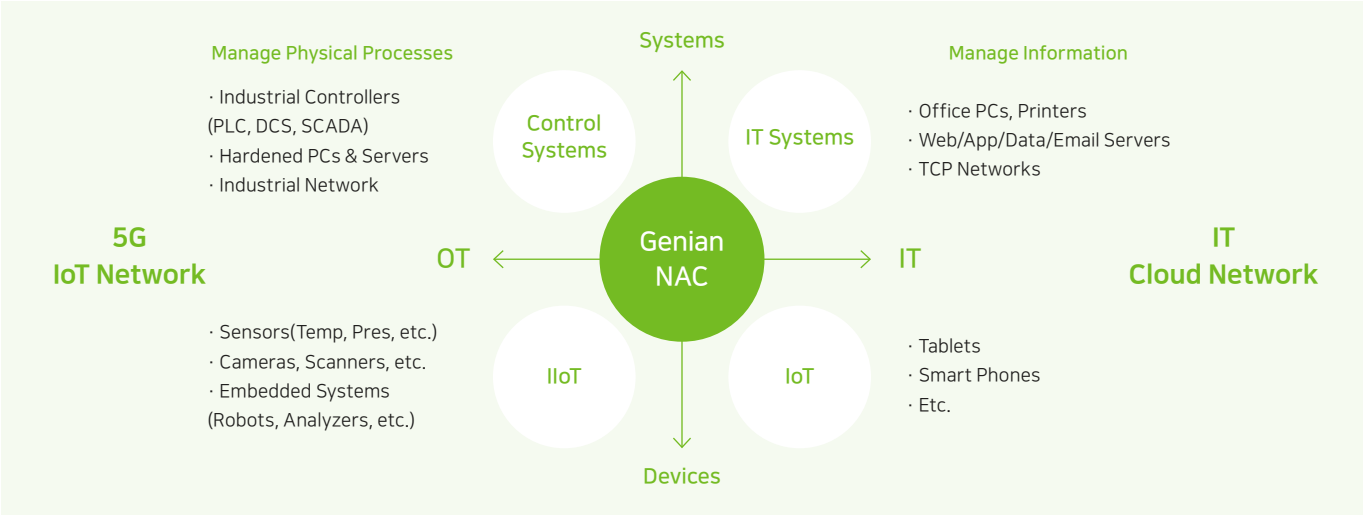
Genian NAC

Overview

네트워크는 더욱 복잡해지며 동시에 확장되고 있습니다. 5G와 Cloud 그리고 IoT(사물인터넷) 등의 발전은 이러한 변화를 더욱 가속화할 것입니다. 기업의 네트워크는 더 이상 데스크톱과 스마트폰의 전유물이 아닙니다. 참여자 역시 내부 직원뿐 아니라 다양한 외부 직원이 함께 근무하고 있습니다. 네트워크의 경계 또한 사라졌습니다. 클라우드 서비스는 보편화되었고 폐쇄망에서도 원격지(remote) 접속이 요구되고 있습니다. 네트워크 환경은 그 어느 때보다 역동적(Dynamic)으로 변하고 있습니다.

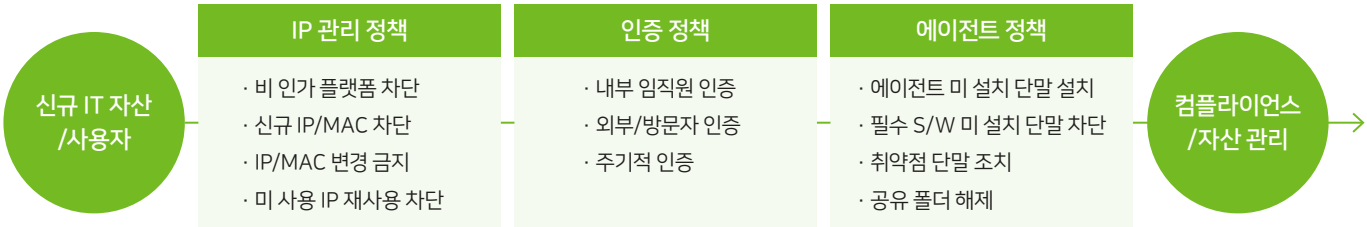
보안 요구 사항 역시 더욱 복잡해지고 있습니다. 환경이 변해도 보안 수준은 유지되어야 하기 때문입니다. 보안 솔루션은 이러한 환경의 변화를 적극 수용해야 하며, 어떠한 상황에서도 본연의 보안 기능을 수준 높게 유지, 제공할 수 있어야 합니다.

Genian NAC는 이러한 변화에 대응할 수 있는 가장 진보된 NAC 솔루션 입니다. IT/OT에 특화된 단말 식별 기술(DPI: Device Platform Intelligence)과 표준 유/무선 통합 인증, 강력한 통제와 다양한 관리기능이 유기적으로 조합되어 지속적으로 상황을 파악하고 실시간으로 통제 및 조치를 수행합니다.



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
- 역할 기반 접근통제(RBAC: Role Based Access Control)
- 표준 802.1X 지원(RADIUS) 및 Dynamic Vlan제공
- DHCP 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
- CISCO/ORACLE/MYSQL/DB2/Tibero/Altibase/CSV 등 연동
- V3 등 백신 및 Palo Alto Networks, Fireeye 제품과 연동

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
- 악성코드 탐지 기능(Malware Detection) 제공

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

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

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)
· 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)	· 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)	· 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)

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 없는 환경에서도 다양한 방식으로 접근 제어

Agent

OS	구분	세부 정보
Windows	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
	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	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
	위 변조 탐지	IP, MAC clone 탐지/차단
	AP 탐지	무선 AP 탐지 및 접속 제어
Windows, macOS, Linux	시스템 정보	PC OS 및 H/W 정보(CPU, MEM, DISK, NIC 등), 호스트명 수집 및 제어
macOS	macOS 업데이트	macOS 자동 업데이트 기능 제공
	장치 제어	USB, NIC, Bluetooth, Wifi, Tethering
	보안 기능	화면보호기 제어, 무선랜 제어 , 에이전트 인증창, 프로세스 제어, 호스트명 변경

Key Features

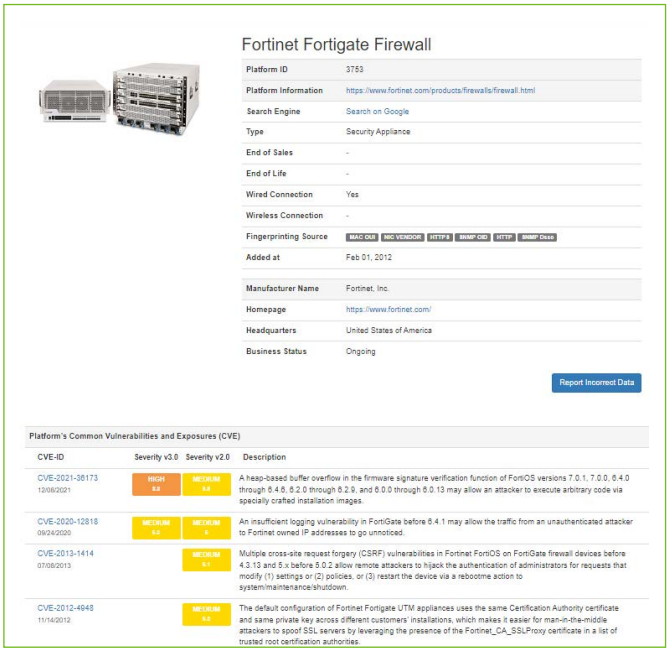
가시성 확보

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.

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

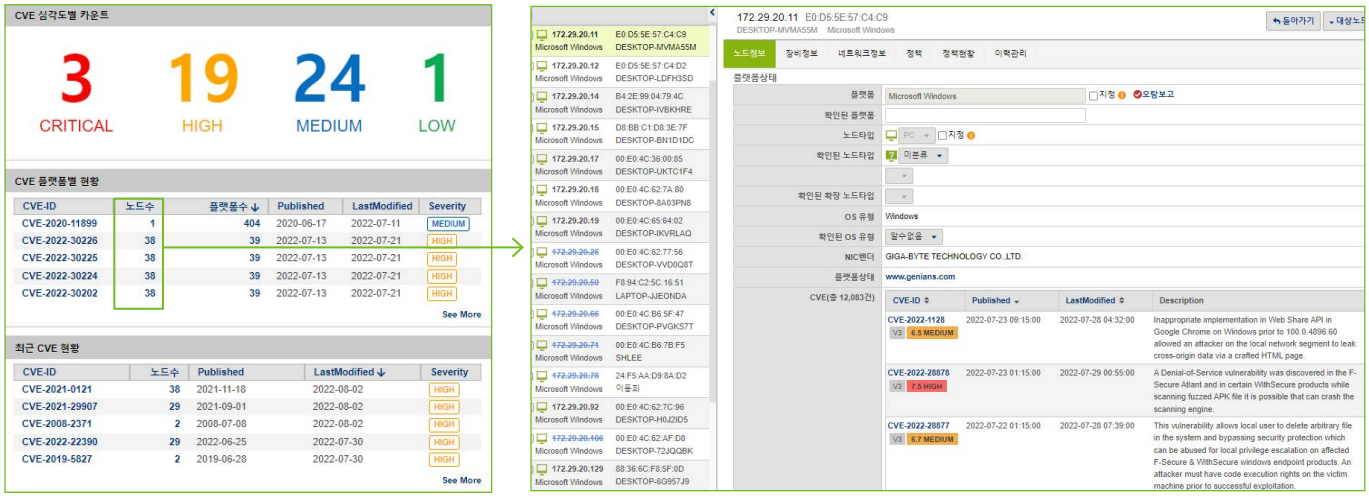
DPI가 제공하는 단말 관련 정보



DPI를 이용한 'Fortinet' 단말 확인

단말 취약점(CVE) 관리

네트워크에 존재하는 단말 관련 취약점 정보를 확인할 수 있습니다. 신규 취약점이 발표되는 경우 해당 단말을 빠르게 찾아 조치할 수 있으며, 향후 에이전트에 의한 자동 패치 적용 등이 지원될 예정입니다.



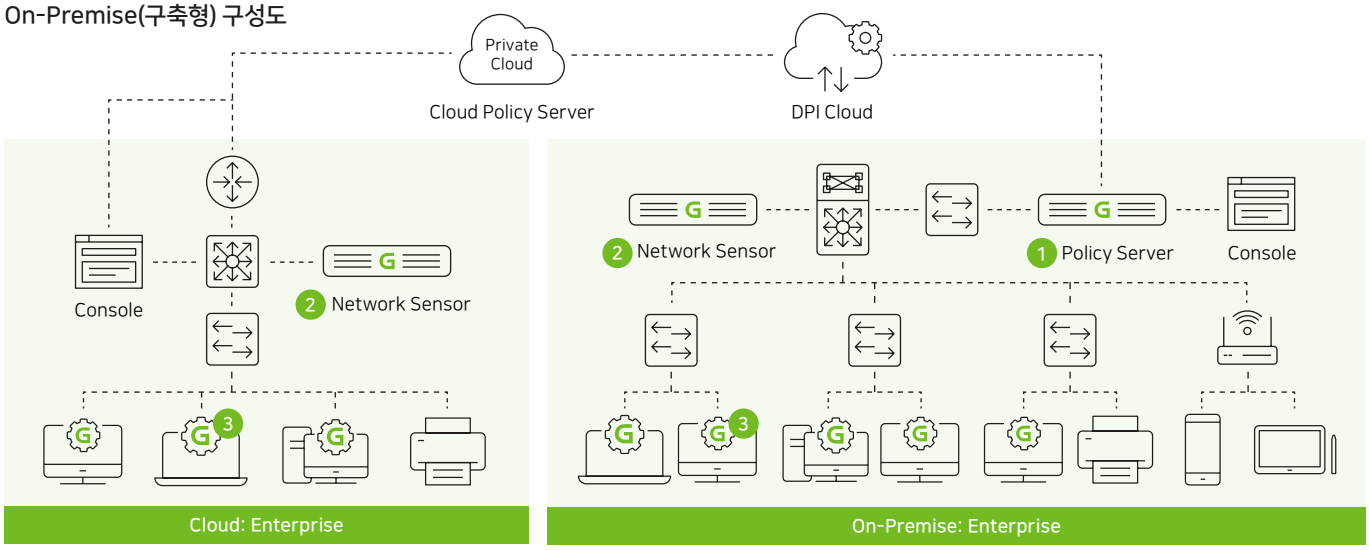
Operating Mode

구성 방안

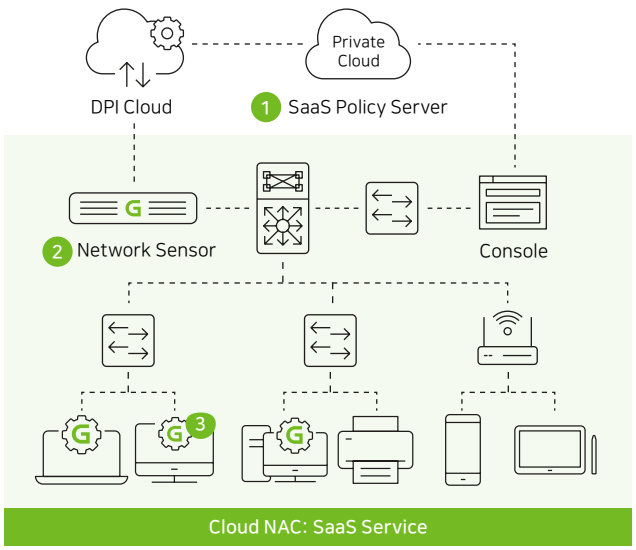
형태 및 목적에 따른 다양한 설치 및 운영 방법을 제공합니다.

On-Premise(구축형)	Cloud(SaaS)	VM(가상머신 등)
· 기관 및 기업의 독자적인 운영 가능 · 국내 환경에 가장 적합 · 고객사에서 가장 선호하는 형태	· 국내 보안 솔루션 최초 클라우드 서비스 보안인증(CSAP)을 받은 제품	· 서비스 사업자를 위한(MSP, MSSP, CSP, SaaS 등) 다양한 플랫폼 및 운영환경 지원 · VM, uCPE, WhiteLabeld 등 포함

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)

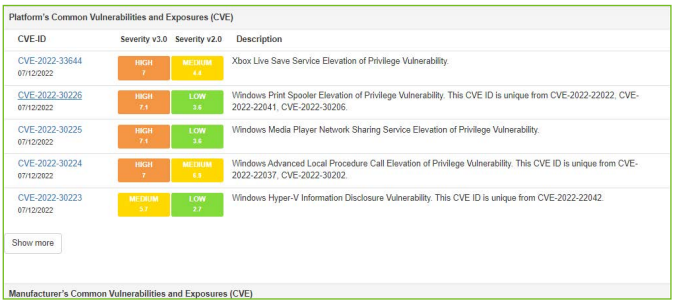
PC 등 에이전트 설치 단말에 자산 관리 및 장치사용 통제,
에이전트 설치에 따른 비용 부담 없음(필요에 따라 선택적 사용)

운영 환경

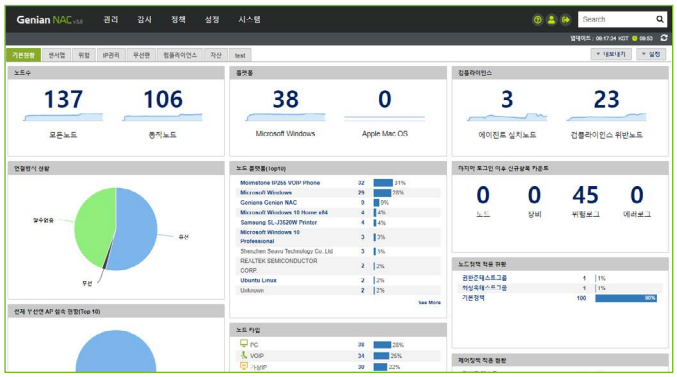
* 상세한 내용은 Genian NAC v5.X Datasheet를 참조하십시오.

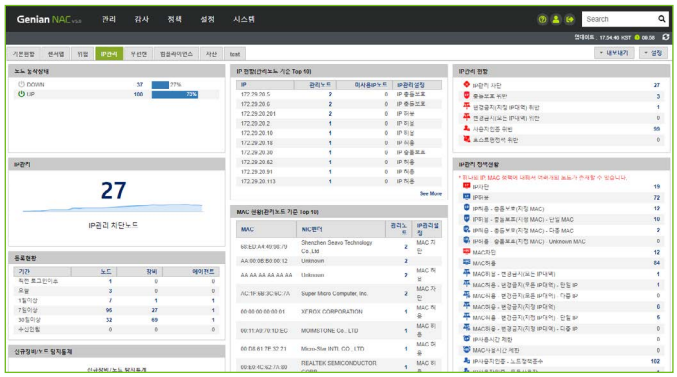
구분	Policy Server(정책서버)	Network Sensor(차단센서)	Agent(에이전트)	Console(콘솔)
사양	전용 어플라이언스(범용 OS)	전용 어플라이언스(범용 OS)	Windows XP 이상/ Mac OS X 10.9 Mavericks 이상/Linux(Debian, RedHat, openSUSE)	MS Edge 40.x 이상/ Chrome 75.x 이상/ Firefox 14.x 이상/ Safari 12.x 이상/IE 10.X 이상

Adminstrator UI

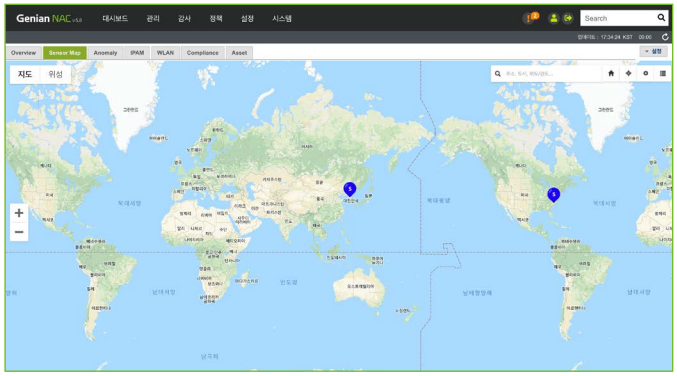


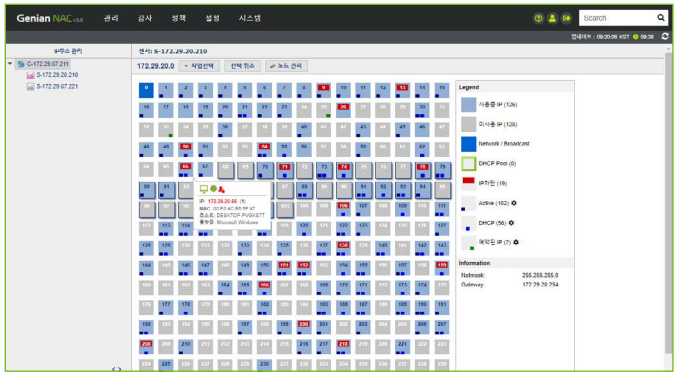
DPI(Device Platform Intelligence)



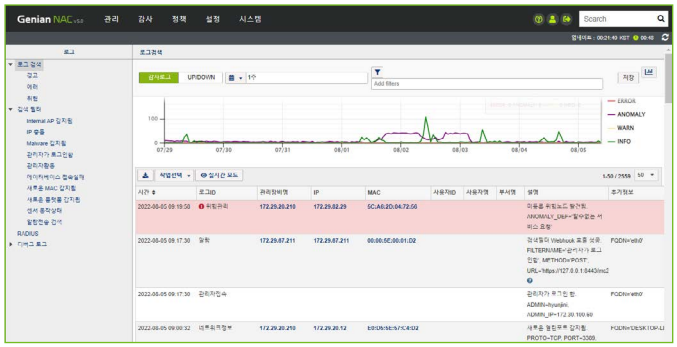


위젯(Widget) 기반 대시보드





센서맵과 IP 매트릭스 뷰



감사(Audit) 및 일간 보고서

조달 디지털서비스몰

NAC 물품식별번호

다량납품 할인율
- 350,000,000 이상 2.5% 할인
- 500,000,000 이상 5% 할인

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↑)	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

나라장터종합쇼핑몰: http://shopping.g2b.go.kr/

14058 경기도 안양시 동안구 벌말로 66 평촌역 하이필드 지식산업센터 A동 12층
기술지원: 1600-9750(평일 오전 9시~오후 7시) / 도입문의: sales@genians.com

Genians