Genian NAC v5.X

Next-Gen Network Access Control for the IoT Era

지니안 NAC는 IoT 환경을 위한 관리와 보안의 핵심입니다.
사용자 뿐 아니라 네트워크에 존재하는 유/무선의 모든 IP 단말을 실시간으로 탐지하고 정확하게 분류합니다. 500개 이상의 다양한 기준으로 탐지된 단말을 분류하고 효과적인 관리와 안전한 보안관리 업무를 수행할 수 있습니다.

HIGHLIGHTS

- 1등 NAC 솔루션
  10년 이상의 연구개발, 조달 점유율70% (Y18/17), 1600여 고객사
- 유/무선 통합 인증
  Portal Login(CWP), 802.1X(RADIUS), AD(LDAP), SAML 등 지원
- IP 관리 (IPM)
  상용 IP 관리 솔루션 수준의 IP신청프로세스 및 인사DB연동을 통한 IP 실명제 지원
- 패치관리 (PMS)
  WSUS내장으로 Windows 및 Office 등 주요 제품군의 패치 및 일반파일 배포기능 지원, 망분리 환경 지원
- 자산관리 (DMS)
  DPI를 이용한 IP 유/무선 단말 탐지 및 Agent 기반 H/W 및 S/W 상세 정보 수집 및 관리
- 접근통제
  역할기반접근통제(RBAC) 및 L2/L3(802.1X), DHCP, Port Mirroring 등 다양한 통제 기능 제공
- 무선관리 (WLAN)
  모든 SSID의 탐지 및 단말 접속 현황 제공, 비 인가 접속장치(Rogue AP) 탐지 및 연결 차단, EAP 지원
- IT Security automation
  직원, 방문자, 특정 단말의 사용을 위한 온보딩(Onboarding) 프로세스 지원 및 등록, IP 등 자원 할당

COMMON CRITERIA · IPv6 FORUM · 1등급 GOOD Software

CHALLENGES

IoT 단말의 홍수 (IoT Tsunami)

보안 관리의 핵심은 단말입니다. OA 단말을 넘어 CCTV 등 IoT 단말이 빠르게 증가하고 있습니다. 공격은 단말을 경유하고 피해는 단말에서 발생하고 있습니다. 단말의 증가는 공격범위(Attack Surface)의 확대를 의미합니다.

제한된 가시성 (Limited Visibility)

단순한 정보로는 충분하지 않습니다. PC, 스마트폰 등의 정보만으로는 정교하고 유연한 관리와 보안정책의 수립 및 운영이 어렵습니다. 플랫폼 정보 뿐 아니라 제조사, 상세사양, 판매여부, 취약점 정보 등 단말의 포괄적 정보가 요구되고 있습니다.

협업과 통제

원격지 사용자와 클라우드 등 네트워크는 더욱 넓어지고 있습니다. 단일한 제품과 단순한 통제만으로는 대응이 불가능합니다. 다양한 보안제품과의 연동은 필수이고 기존 인프라와의 통합이 필요합니다.

KEY FEATURES

디바이스 플랫폼 인텔리전스 (DPI: Device Platform Intelligence)

단말 가시성 확보를 위한 가장 진보된 방법으로 IP 단말을 대상으로 식별정보/확장정보/위협 정보를 동시에 확인할 수 있습니다.

- 식별정보 : 제조사/이름/모델번호/사진/상세정보 URL 등
- 확장정보 : 제조사 URL/본사위치/사업여부/판매종료/지원종료 등
- 위협정보 : 단말 및 제조사 취약점 정보(CVE No/Severity/Description)

* Policy Server의 인터넷 연결이 필요합니다.

국내 최다 연동 및 협업

인사정보DB, AD(Active Directory) 뿐만 아니라 ORACLE, MYSQL. MSSQL/Sybase, IBM DB2, TIBERO, ALTIBASE, PostgreSQL, LDAP, CSV, CUBRID 등과 연동이 가능합니다. 차세대 방화벽, 침입방지 시스템 등 40여 보안 솔루션과 연동 및 협업이 가능하며 RESTful API, Syslog, Webhook, SNMP trap 등을 지원합니다.

악성코드 탐지 (Malware Detection)

에이전트가 설치된 단말의 정보를 수집하여 악성코드를 탐지합니다. 상용 지니안 Insights E 에 적용된 머신러닝 기반 탐지로 백신 등 시그니처 제품이 탐지하지 못하는 악성코드를 탐지 할 수 있습니다.

COMPONENTS & DEPLOYMENT

지니안 NAC는 Policy Server/Network Sensor/Agent(선택)로 구성됩니다. 각 구성요소의 역할과 동작은 기존 인프라에 미치는 영향을 최소화하도록 설계되었습니다. Out-of-Band 동작 방식은 네트워크 성능에 영향을 주지 않으며 장애 시에도 네트워크 영향을 최소화합니다. Agent 역시 차단이 아닌 정보 수집을 주 목적으로 개발되어 PC 등 단말의 영향을 최소화합니다.

Policy Server & Console (정책서버 & 콘솔)

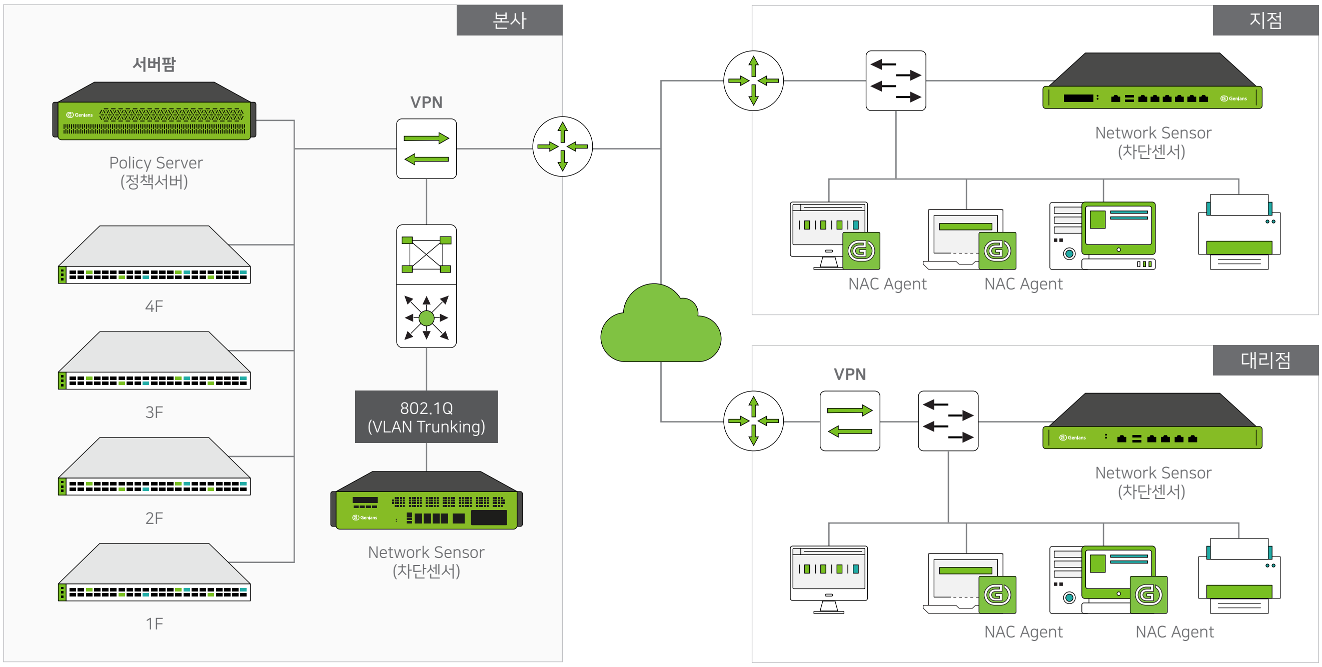
- DPI 기반 유/무선 단말 관리
- 인증, 통제, 허가 등 보안정책 수립 및 통제

Network Sensor (차단센서)

- 네트워크 및 유/무선 단말 탐지
- 네트워크 통제

Agent (에이전트, 선택사항)

- 단말에 설치되어 정보 수집 및 장치(USB 등) 사용 통제
- 비용 부담 없으며 선택적 사용



Genian NAC 구성

SPECIFICATIONS

Policy Server & Console (정책서버 & 콘솔)

- 자체 OS(이중화 및 DB 분리 구성 지원)
- 전용 어플라이언스 외 클라우드(AWS), COTS(Commercial off-the-shelf), VM, Docker 등 지원 *
- 표준 브라우저 지원(익스플로러, 크롬, 파이어폭스 등)

Network Sensor (차단센서)

- 유선: 자체 OS(이중화(HA) 구성 지원/802.1q, 802.1ad Trunking, Bonding Port 지원)/In-Line 지원
- 전용 어플라이언스 외 COTS, VM, uCPE(Universal Customer Premise Equipment) 등 지원 *

Agent (에이전트)

- Windows XP 이상/Mac OS X 10.9 Mavericks 이상/Linux(Debian, RedHat, openSUSE)

* 상세한 정보는 별도 자료 'Solution Brief_Genian NAC for SP(Service Provider)'를 참고하십시오.

MAIN FEATURES

CATEGORY	FEATURES
가시성 (단말의 탐지 및 식별)	IP 보유 유/무선 단말의 탐지(IPv4 / IPv6)
	DPI(디바이스 플랫폼 인텔리전스) 기반 단말 상세 정보 제공 (단말 종류, 운영체제 식별/단말 타입 자동감지/탐지된 플랫폼의 EOL, CVE 정보 제공)
	Active/Passive Scan 지원
	스위치(Switch) 포트 정보 수집
	무선랜(WLAN) 모니터링/비 인가(Rogue) Access Point 탐지
	WMI 지원/OS, H/W, S/W, 시스템 리소스(CPU, MEM 등) 등 정보 수집(Agent 설치 시)
	조건에 따른 단말 분류(500가지 이상)
	위젯(100가지 이상) 기반 맞춤형 대시보드
	변경사항 추적/감사 로그
	네트워크 이상징후 탐지(MAC Spoofing, Rogue Gateway, Ad-hoc 등)
	기본 리포트 제공(Node, WLAN, Log 등)
	고객 맞춤형 리포트 제공 가능
사용자 인증	CWP(Captive Web Portal) 사용자 인증
	Active Directory SSO 인증 정보 연동
	LDAP, SMTP, POP3, IMAP, SAML(Google G Suite 등) 등 외부 인증 연동
	802.1x 인증을 위한 RADIUS 서버 기능
	사용자/부서/직급 등 인사DB 연동(Oracle, MySQL, PostgreSQL, MSSQL, LDAP, CSV 등)
	지문인식 지원(Suprema, Nitgen)
	외부 OTP 인증 연동(ANYOTP, Google OTP)
네트워크 접근 제어	역할기반 접근 제어(RBAC)
	ARP 기반 Layer 2 제어
	802.1x 기반 제어(RADIUS Server)
	포트 미러링 기반 제어
	스위치 통합 기반 제어(Switch Port Shutdown)
	비정상 단말의 DHCP 할당 제한
	기타 보안 위협 수준에 따른 30여 제어기능 제공(경고/차단/격리 등)
데스크탑 관리	보안정책 준수 점검(AV 사용, 최신 패치적용, 필수S/W 설치 여부 등)
	운영체제 환경설정(화면보호기, DNS 설정 등)
	운영체제 업데이트
	장치 제어(USB, DVD-RW 등)
	802.1x 연결 관리
	WLAN 탐지 및 제어(SSID 설정, 핫스팟(SoftAP) 차단 등)
패치 및 소프트웨어 관리	패치 설치 대상 및 승인여부 관리
	패치 적용 시점 지정(즉시, 종료시, 시간대 등) 및 백그라운드 설치
	독립 배포서버 구축(폐쇄망 및 오프라인 패치 지원)
	사용자 별 패치 상태 정보 제공
	관리자 지정 소프트웨어 배포 및 설치(백신 등)
	규정 위반 소프트웨어에 대한 원격, 강제 삭제
취약성 관리	버전, 업데이트 등 주요 백신 13종 정보수집(V3, 알약, Symantec, Trend Micro 등)
	V3, 알약 등 4대 백신 연동(강제 검사, 업데이트 등 지원)
	탐지된 단말의 취약성 정보(CVE) 확인 지원
	Agent 설치 단말에 대한 악성코드 탐지(Malware Detection) 기능
외부 연동	User Directory 연동(RDBMS, LDAP)
	외부 연동을 위한 Syslog/REST API/Webhook/SNMP trap 등 지원
비즈니스 프로세스	단말 연결 시(보안서약 등) 동의(consent) 페이지 노출 및 통계 정보 제공
	신청 프로세스 지원(IP, 단말, 사용자, 매체에 대한 다단계 신청/승인 등)
	관리자 역할(Role)에 따라 서로 다른 콘솔 지원
	목적에 따른 다중 CWP(Captive Web Portal) 지원
	다국어 지원 (한국어/영어/일어)
확장성과 가용성	이중화 구성 지원 (Policy Server/Network Sensor)
	NIC(Network Interface Card) Channel Bonding 지원
	DR (DB Replication/Policy Server Backup 등) 지원
기타	Mobile App 지원(Android/iOS 지원)
	IPv6 Ready(Phase 2)

APPLIANCE LINE UP

Policy Server & Console (정책서버 & 콘솔)

모델	C10_R1	C20_R1	C30_R1	C40_R1	C50_R1
					
CPU	Intel Celeron 2.8G (2Core)	Intel I3 3.7G (2Core)	Intel E3 3.3G (4Core, Xeon)	Intel E3 3.6G (4Core, Xeon)	Intel E5 2.1G (8Core, Xeon)
Memory	8GB	8GB	16GB	16GB	32GB
HDD/SSD	500GB/64GB	1TB/64GB	1TB/64GB	1TB/256GB	1TB/256GB
Port	4	2	2	2	2
Node	1,000	4,000	8,000	12,000	20,000

Network Sensor (차단센서)

모델	S10_R1	S20_R1	S20H_R1	S30H_R1	S40H_R1	S50H_R1
						
CPU	Intel Celeron 2.41G(2Core)	Intel Celeron 1.99G(4Core)	Intel Celeron 1.99G(4Core)	Intel Celeron 2.8G(2Core)	Intel I3 3.7G(2Core)	Intel E3 3.3G(4Core)
Memory	2GB	2GB	2GB	4GB	8GB	8GB
HDD/SSD	-	-	500GB	500GB	1TB	1TB
Port	2	4	4	4	6	8(4)
Node	100	250	350	1,000	2,000	3,000

CONTACT US

문의 및 데모요청 : sales@genians.com
장애지원 및 기술문의 : support@genians.com
본 자료 및 내용문의 : mkt@genians.com

Genians

Next-Gen Network Access Control for the IoT era

2005년 1월 설립된 지니언스(www.genians.com, 코스닥 종목번호 263860)는 기술개발을 선도하며 글로벌 비즈니스 확장을 통해 보안 SW 전문기업으로 성장하고 있습니다. 인증 및 식별 그리고 접근제어 분야 특화된 기술을 바탕으로 국내 1등 NAC 솔루션을 보유하고 있으며, 시장을 선도하고 있습니다. 2017년 단말 기반 지능형 위협 탐지 및 대응 솔루션 '지니안 인사이즈 E(Genian Insights E)'를 출시하며 EDR 시장에 진출 했습니다. 2016년 1월 해외사업 시작과 함께 미국 보스턴에 현지법인을 설립한 바 있으며 2017년 8월 코스닥에 상장했습니다.