Data Sheet

Genian NAC v 5.X

Genian 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.

Highlight

사용자 인증 관리
- Portal Login(CWP), 802.1X(RADIUS), AD(LDAP), SAML 등 지원

IP 관리 (IPAM)
- 상용 IP 관리 솔루션 수준의 IP 신청 프로세스
- 인사 DB 연동을 통한 IP 실명제 지원

패치 및 소프트웨어 관리
- WSUS 내장으로 Windows 및 Office 패치 관리
- 일반파일 배포 및 설치 지원

자산 관리(DMS)
- DPI를 이용한 IP 유/무선 단말 탐지
- Agent 기반 H/W 및 S/W 상세 정보 수집 및 관리

네트워크 접근 제어
- 속성 기반 접근통제(ABAC)
- DHCP, Port Mirroring 등 다양한 통제 기능 제공

무선 네트워크 접근 제어
- SSID별 단말 접속 현황 파악
- 비 인가 접속장치(Rogue AP) 탐지 및 연결 차단
- 무선 접속 매니저(EAP-GTC) 지원

IT Security Automation
- 직원, 방문자, 특정 단말의 사용을 위한 온보딩(Onboarding) 프로세스 지원 및 등록, IP 등 자원 할당

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.

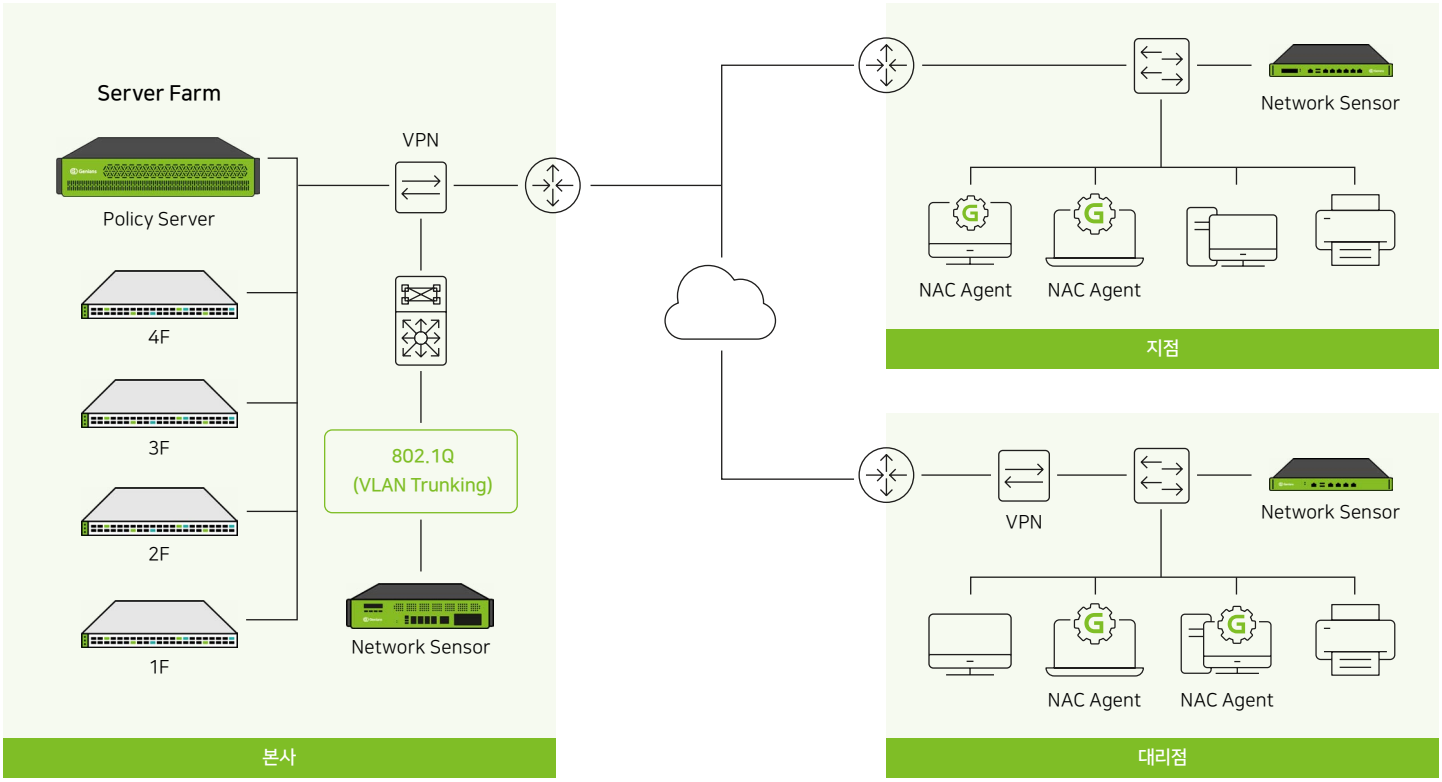
악성코드 탐지(Malware Detection)
에이전트가 설치된 단말의 정보를 수집하여 악성코드를 탐지합니다.
상용 Genian EDR에 적용된 머신러닝 기반 탐지로 백신 등 시그니처 제품이 탐지하지 못하는 악성코드를 탐지 할 수 있습니다.

Components&Deployment

Genian 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	Network Sensor	Agent(선택사항)
· DPI 기반 유/무선 단말 관리 · 인증, 통제, 허가 등 보안정책 수립 및 통제	· 네트워크 및 유/무선 단말 탐지 · 네트워크 통제	· 단말에 설치되어 정보 수집 및 장치(USB 등) 사용 통제 · 비용 부담 없으며 선택적 사용

Genian NAC 구성



Specifications

Policy Server&Console	Network Sensor	Agent
· 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 (Chrome, Firefox, Safari 등)	· 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*	· Windows XP 이상/ Mac OS X 10.9 Mavericks 이상/ Linux(Debian, RedHat, openSUSE)

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

Product Funtion

Category	Features
네트워크 접근 제어	속성 기반 접근통제(ABAC: Attribute Based Access Control)
	표준 802.1X 지원(RADIUS) 및 Dynamic Vlan 제공
	DHCP 서버 내장 및 할당 제어
	ARP 기반 Layer 2 지원
	포트 미러링 및 방화벽/스위치 통합 기반 제어
사용자 인증 관리	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 Vlan 지원
	LDAP, SMTP, POP3, IMAP 등 외부 인증 연동
	SAML(Google G Suite, Okta) 인증 연동
	지문인식 및 OTP(Google OTP 등) 연동
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
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
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
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
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
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)

Appliance Line Up

Policy Server&Console

모델명	C10_R1	C20_R1	C30_R1	C40_R2	C50_R2
모델 이미지					
CPU	Intel Celeron 2.8G (2Core)	Intel I3 3.7G (2Core)	Intel E3 3.3G (4Core, Xeon)	Intel E 3.7G (6Core,Xeon)	Intel E5 2.2G (10Core, 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	5,000	10,000	20,000	30,000

Network Sensor

모델명	S10_R2	S20_R2	S20H_R1	S30H_R1	S40H_R1	S50H_R1
모델 이미지						
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	-/32GB	-/32GB	500GB/-	500GB/-	1TB/-	2TB/-
Port	2	4	4	4	6	8(4)
Node	100	250	500	1,000	2,000	3,000

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

Genians