



**Genian** Cloud NAC



Genian  
NAC

01

개요

03

Cloud NAC ?

03

Cloud NAC 제품 소개

04

회사 소개

The logo for Genian NAC is a stylized, multi-layered shape with a color gradient from light green to dark teal. The text "Genian" is positioned above "NAC" in a white, sans-serif font.

Genian  
NAC

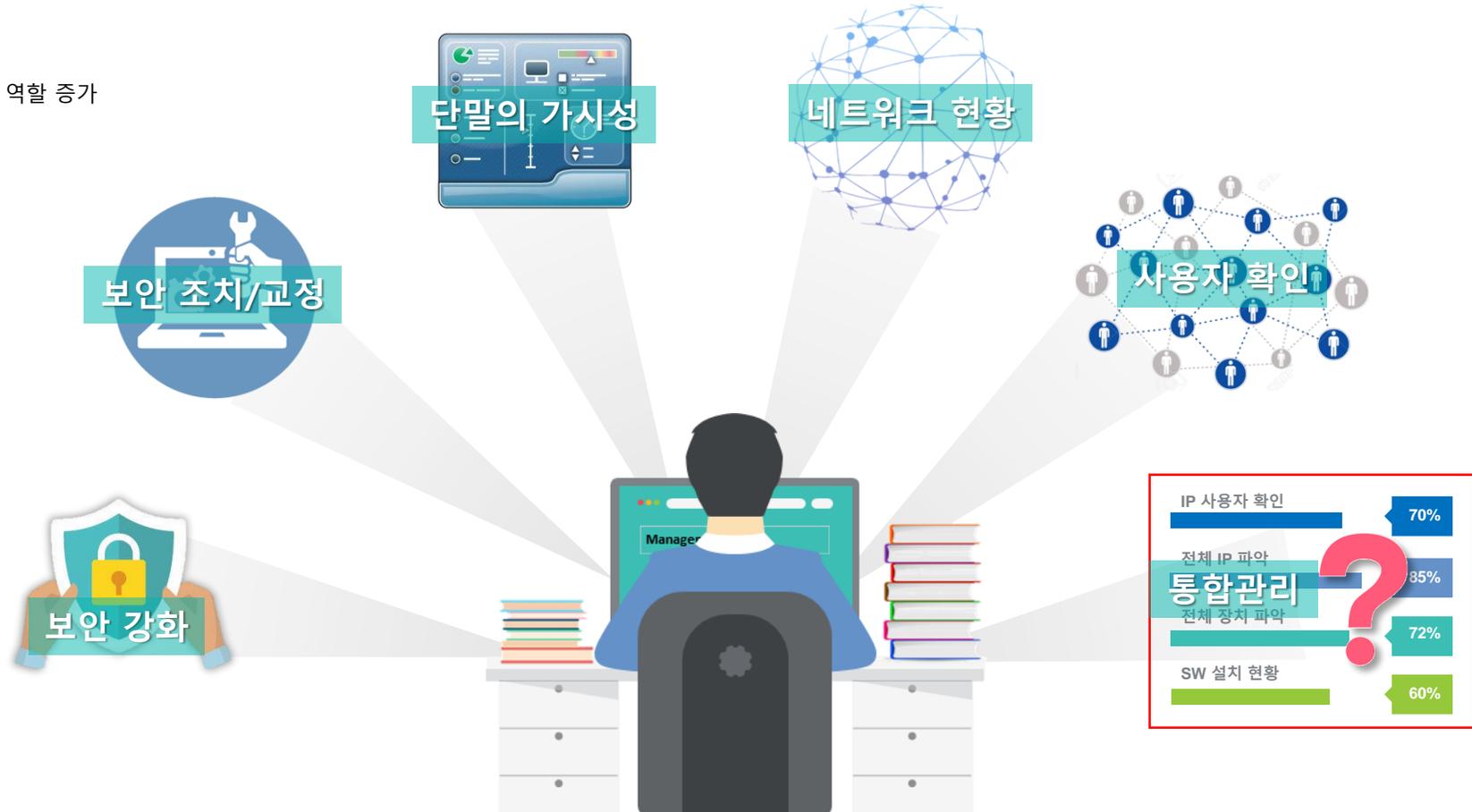
---

개요

---

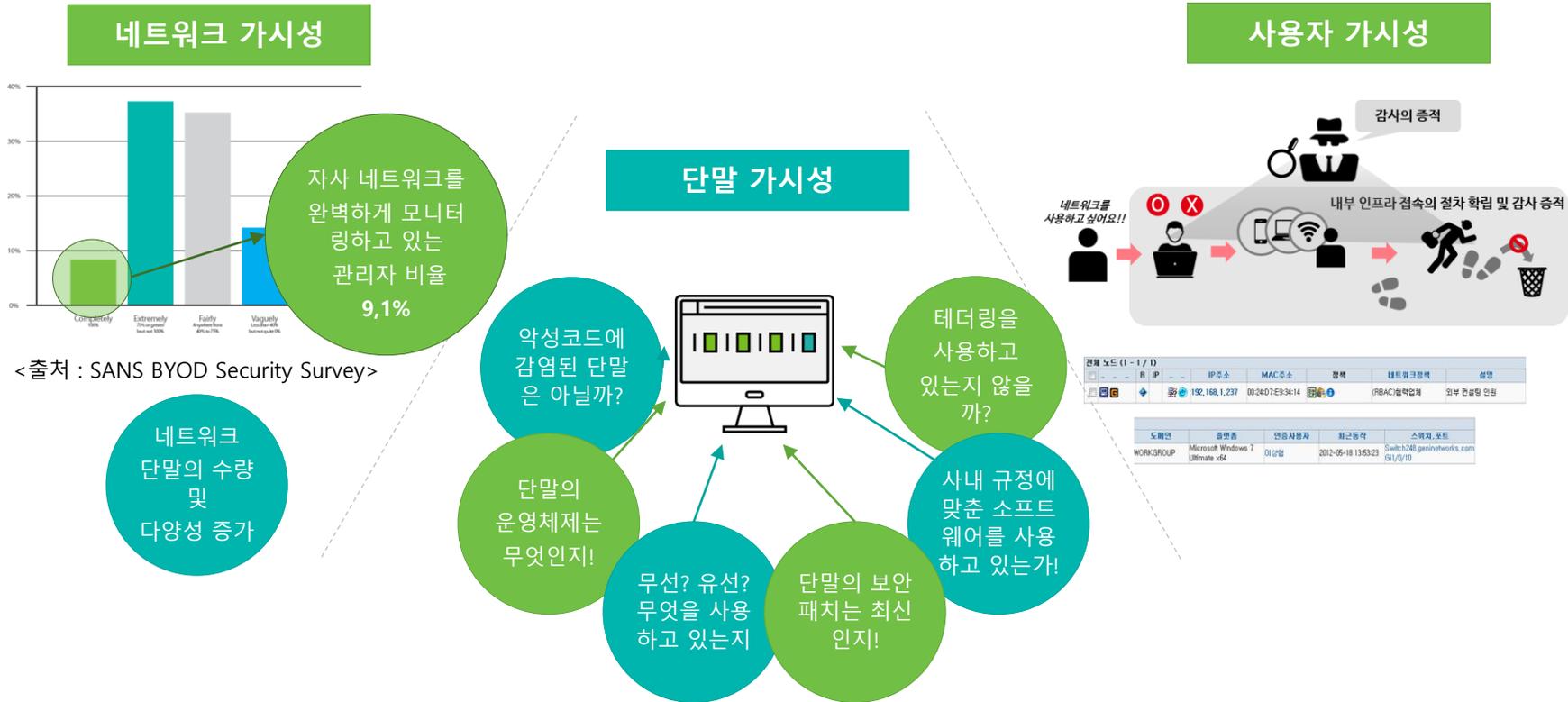
## - 관리 부서의 고민

- 지속적인 보안사고로 인한 관리부서(자)의 역할 증가



## - 내부보안? 가시성(Visibility) 확보!

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





---

Cloud NAC ?

---

### - Cloud NAC 이란?

- 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



### Cloud 기반 통합 관리

- 고객사 단말기 현황 파악 및 통합 관리 시스템 구축
- 다수의 고객을 동시에 관리할 수 있는 Cloud 기반 관리 서버 제공



## - Cloud NAC 장점 (1/2)

- 기존 On-premiss NAC 대비 저렴한 초기 도입 비용
- 정책 서버 설치가 필요 없는 간편한 설치
- 내부 관리자가 없는 환경에서도 장애 지원 및 유지 보수 가능

	On-Premise NAC	Cloud NAC
도입 비용	Appliance (Policy Center) 장비 구매 비용 필요	별도의 Appliance (Policy Center) 장비 구매 필요 없음
설치	물리적인 Policy Center와 Network Sersor 모두 설치	Network Sersor 장비 설치
유지 보수	내부 관리자의 직접 관리 필요	내부 / 외부에서 관리 가능



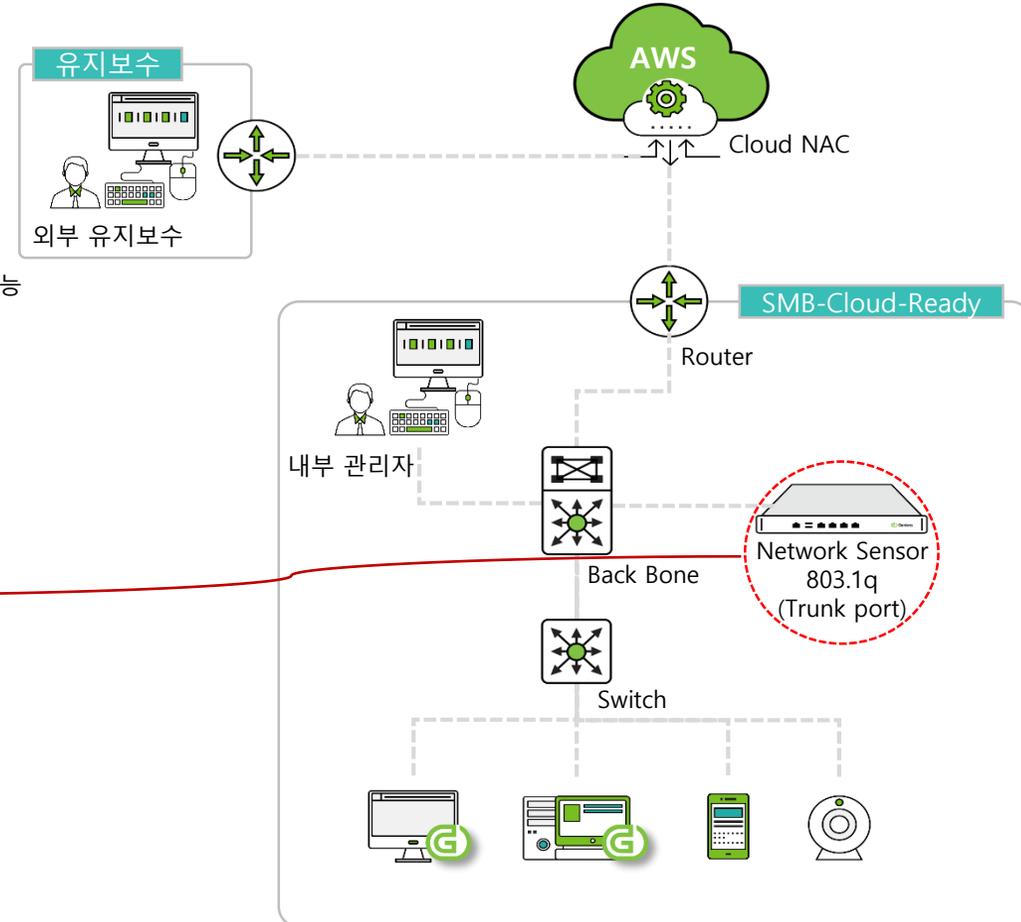
## - Cloud NAC 장점 (2/2)

- 다양한 플랫폼 및 운영환경 지원

Cloud-Ready (AWS 또는 서비스 프로바이더)			
Cloud	전용 Appliance docker	가상 머신(VM)	White Labeled
구분	지원 플랫폼	세부 지원 사양	
① 정책서버 (Policy Server)	CLOUD	AWS, AZURE(US, Korea, Singapore Region)	
	COTS(Commercial Off-The-Shelf)	Intel Server (HP, DELL)	
	가상머신(VM)	VMWARE, KVM	
	컨테이너	DOCKER	
	White Labeled	사업자 전용 H/W	
② 차단센서 (NetworkSensor)	전용 Appliance	X86기반 임베디드(Custom OS + Network Sensor)	
	COTS	MiniPC, (Intel NUC)	
	가상머신(VM)	VMWARE, KVM	
	uCPE (Universal Customer Premise Equipment)	Lanner	

## - Cloud NAC 구축 예시

- Policy Center는 Cloud 환경인 AWS에 구성되어 있어 내부 환경 내 별도 설치가 필요 없음
  - Network Sensor의 경우 내부 설치 필요
  - Cloud 환경 특성상 내부 / 외부 어디에서나 관리가 용이함
- ※ Network Sensor의 경우 고객사 내 제공할 수 있는 유휴 장비(서버)에 이미지를 올려서 설치 가능



- Vlan 환경일 경우 Trunk Mode 단일 센서로 관리 가능
  - 라우팅 구간 변경 시 개별 센서 추가 필요
- ※ 구축 진행 전 네트워크 정보 확인 후 구성 필요

### - Cloud NAC 보안 기능

#### - 선택 가능한 관리 및 보안 기능

- NAC 솔루션은 내부 보안과 관리를 위한 다양한 기능을 지원합니다. 이러한 기능은 별도의 전용 솔루션을 대체할 수 있으며 기능 간의 연동을 통하여 관리와 시너지 효과를 극대화할 수 있습니다.
- 고객에게 제공하는 기능은 Service Provider의 요구와 고객의 상황에 따라서 조정이 가능합니다.

#### IPM (IP 관리)

- 독립 솔루션 수준의 IP 관리 기능 제공
- 인사 DB 연동을 통한 IP 실명제
- DHCP 내장 및 신청/승인 등 업무절차 지원

#### AAA (인증 관리)

- 자체 포털(CWP) 사용자 인증 지원
- 802.1X 지원 및 RADIUS 서버 내장
- 기존 인사 DB 및 SAML, OTP, 지문 등 지원

#### DMS (데스크톱 관리)

- 모든 데스크톱의 자동 탐지 및 식별
- 실시간 상세(H/W, S/W, 패치 등) 정보 수집
- '언제, 어디서, 누가, 무엇으로'의 현황 관리

#### PMS (패치 관리)

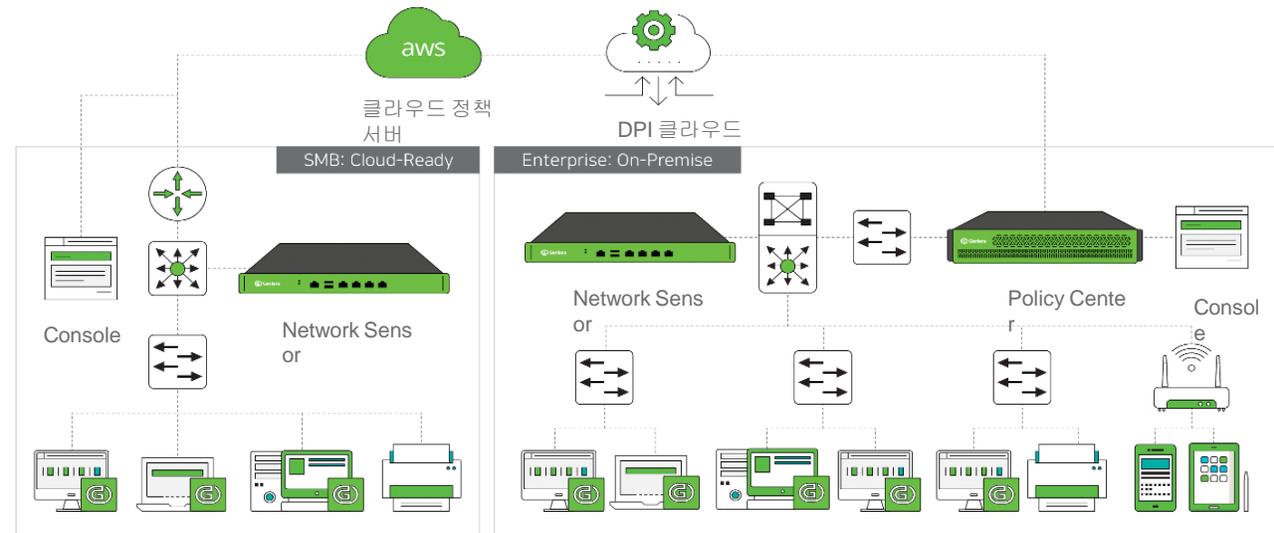
- WSUS 기반 MS Windows 및 Office 패치 관리
- 일반 파일 배포 및 설치 지원
- 망 분리(폐쇄망) 환경 지원

#### WLAN (무선 관리)

- SSID 및 SSID 별 접속 단말 현황 파악
- 불법(rogue) AP 및 SoftAP(핫스팟) 등 탐지
- 무선 접속 매니저 제공 및 802.1X 지원

#### DMS (장치 관리)

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





---

# Cloud NAC 제품소개

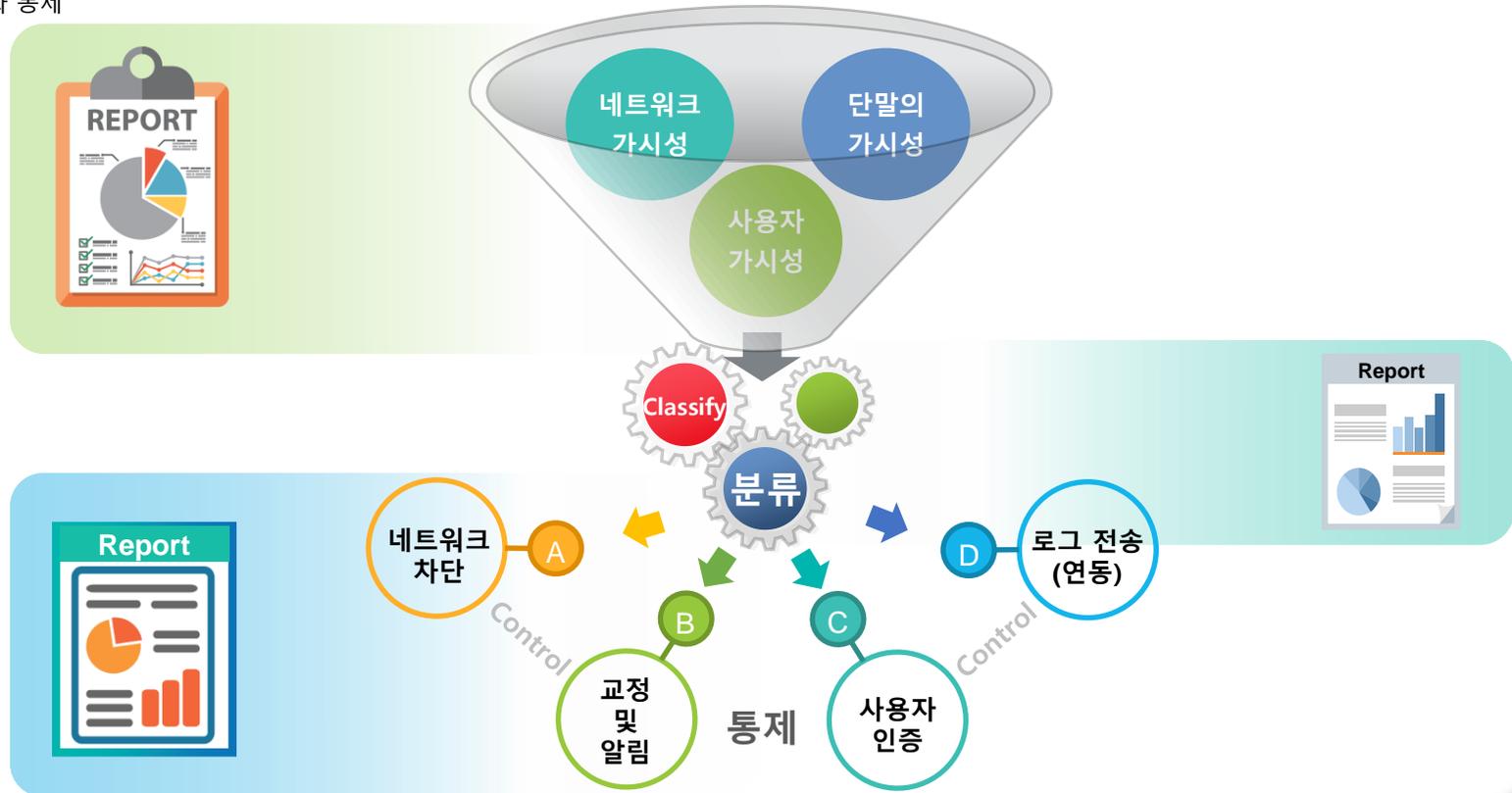
---

# 03

## Cloud NAC 제품 소개

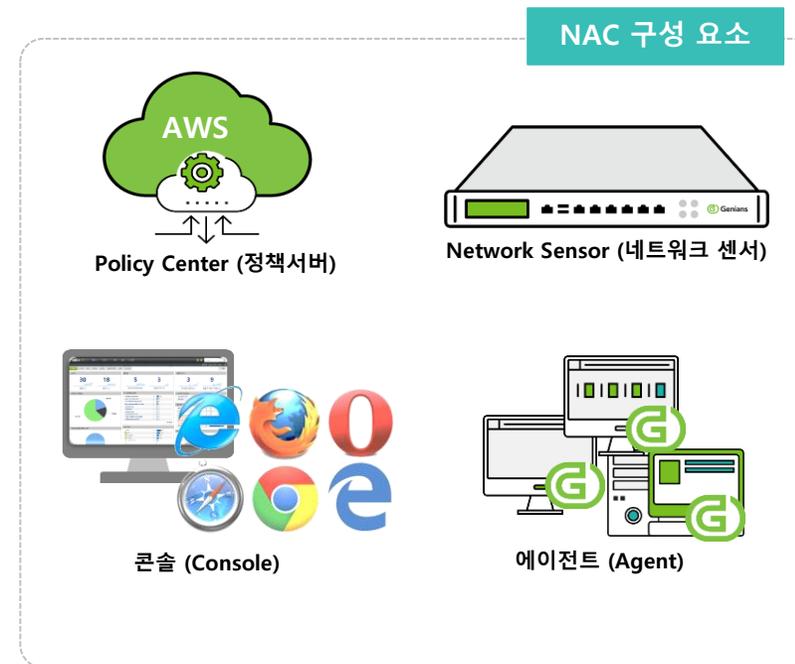
- 관리 툴을 넘어선 필수 인프라 NAC

- 접근 제어의 필수 요소인 다양한 가시성을 통한 분류와 통제



## - Cloud NAC 구성 (1/3)

- ① 정책서버 (Policy Center) - **AWS 환경에서 지원**
  - 유무선 네트워크를 통합 관리하고 내부 보안을 강화할 수 있도록 지원
- ② 차단센서 (Network Sensor) - 사내 유휴 서버 사용, 대여, 구매 등 다양한 방식 지원
  - 유무선 단말에 대한 정보를 수집하고 강력한 통제 수행
- ③ 에이전트 (Agent)
  - PC 등 에이전트 설치 단말에 대한 자산 관리 및 장치사용 통제
  - Agent 설치에 따른 비용 부담 없음(필요에 따라 사용/미사용 가능)
- ④ 콘솔 (Console)
  - 관리자 웹 콘솔
  - IE, Chrome, FireFox, Safari, Opera 등 다양한 환경 지원



# 03

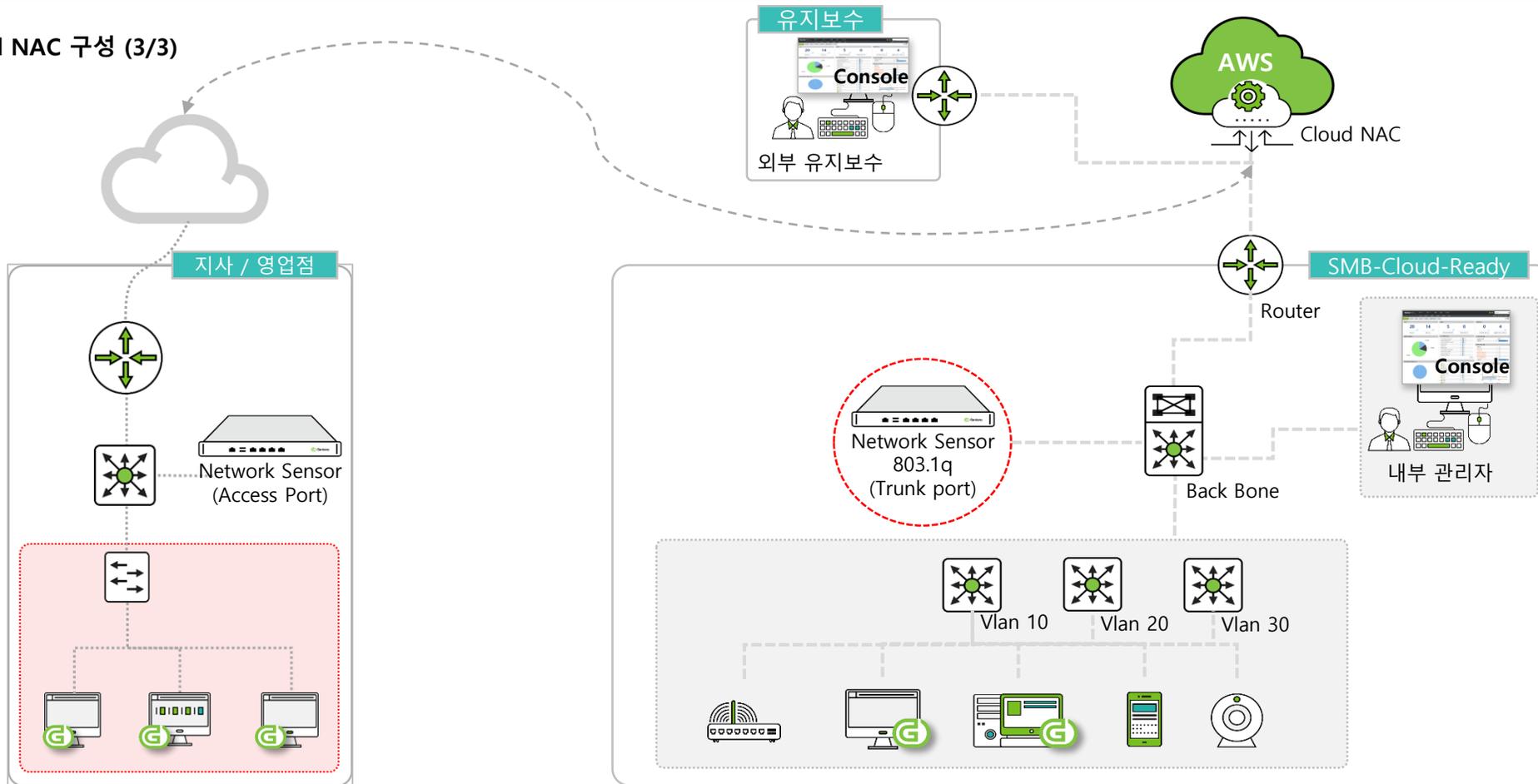
## Cloud NAC 제품 소개

### - Cloud NAC 구성 (2/3)

항목	종류						설명
	100 Node	200 Node	300 Node				
Policy Center (정책 서버)						-	- 보안정책 수립 - 단말 현황 및 이력 관리
Network Sensor (네트워크 센서)	S10_R1 	S20_R1 	S20H_R1 	S30H_R1 	S40H_R1 	S50_R1 	- 유/무선 네트워크 제어 - 네트워크 정보 수집 - DHCP 서비스 제공
Agent (에이전트)	Genian Agent 	-	-	-	-	-	- HW, SW 정보 수집 - 보안 설정 유무 확인 및 교정 - MS patch
Console (관리자 웹 콘솔)	Console 	-	-	-	-	-	- 유무선 네트워크 통합 관리 지원

※ Cloud NAC - AWS 환경의 Policy Center(정책 서버) 제공

## - Cloud NAC 구성 (3/3)



## - 가시성 (1/3)

- 네트워크 내의 모든 단말기 정보 수집 및 분류, IP 실명 확인

장치 구분	On/Off	가동률	인증 정보	인증 시간	연결된 스위치		IP/MAC		사용 위치	OS/장치 모델 상세 정보	서비스	최종연결시간	Hostname	NIC 제조사	동작 현황
					스위치	포트	IP주소	MAC주소							
NTAG SS	동작	22%	활	2018-04-05 15:29:09			172.29.50.158	E4:70:B8:EE:5B:33	50.0 연구소IP대역	Microsoft Windows 10 Home x64	P)		DESKTOP-9KISQBM	Intel Corporate	
	동작	16%	활	2018-04-02 08:38:31			172.29.20.78	00:E0:4C:36:06:99	S-172.29.20.4	Microsoft Windows 10 Home x64	P)		DESKTOP-9KISQBM	REALTEK SEMICONDUCTOR CORP.	
	동작	19%	전	2018-04-04 19:19:44	172.29.50.6	1	172.29.50.228	DC:0B:34:B9:AE:C9	50.0 연구소IP대역	LG Android Device	P)		android-4d2a63951ba29b9d	LG Electronics (Mobile Communications)	
	동작	32%	하	2018-04-04 17:05:28	172.29.50.6	1	172.29.50.229	E8:3A:12:1C:08:D8	50.0 연구소IP대역	Samsung GALAXY S6 Phone	P)	2018-04-04 17:32:52	Android	Samsung Electronics Co.,Ltd	
	동작	2%	하	2018-04-03 12:36:59			172.29.50.219	80:E6:50:0F:5D:B8	50.0 연구소IP대역	Apple MacBook Pro	P)	2018-04-03 09:55:19	MACBOOKPRO-5DB8	Apple, Inc.	
	동작	20%	하	2018-04-02 07:12:12			172.29.20.41	D0:27:88:D9:3C:BE	S-172.29.20.4	Microsoft Windows 7 Professional	P)	2018-04-04 17:28:52	KEVIN	Hon Hai Precision Ind. Co.,Ltd.	
	동작	29%	하	2018-04-02 08:00:22			172.29.20.42	00:E0:4C:39:48:43	S-172.29.20.4	Microsoft Windows 10 Professional x64	P)	2018-04-05 15:03:30	HKHAN	REALTEK SEMICONDUCTOR CORP.	
	동작	20%	한	2018-02-07 14:05:05			172.29.20.58	D0:50:99:91:D3:70	S-172.29.20.4	Microsoft Windows 10 Professional x64	P)		DESKTOP-CR1H8TU	ASRock Incorporation	
	동작	24%	하	2018-04-05 15:18:29	172.29.50.6	1	172.29.50.189	D0:2B:20:89:DA:2B	50.0 연구소IP대역	Apple Device	P)		Playdesignin	Apple, Inc.	
	동작	29%	최	2018-04-02 08:53:49			172.29.126.61	00:E0:4C:69:01:11	126.0(이상훈 책임)	Microsoft Windows 10 Home x64	P)		JUNSU-KNOTEBOOK	REALTEK SEMICONDUCTOR CORP.	
	동작	0%	최	2018-04-02 21:21:18			172.29.250.29	B4:B6:76:77:AA:06	C-172.29.53.150	Microsoft Windows 10 Professional x64	P)	2018-04-02 21:53:13	YOUSINNOTE	Intel Corporate	
	동작	83%	최	2018-03-30 18:35:53			172.29.60.180	40:8D:5C:70:7F:22	60.0 (AGENT팀)	Microsoft Windows 10 Professional x64	P)		DESKTOP-UMVOTUM	GIGA-BYTE TECHNOLOGY CO.,LTD.	
	동작	26%	진	2018-04-05 15:23:31	172.29.50.6	1	172.29.50.199	6C:4D:73:DA:29:09	50.0 연구소IP대역	Apple iPhone	P)	2018-04-05 15:26:34	iPhone8	Apple, Inc.	
	동작	0%	진	2018-04-03 10:24:19			172.29.100.138	AC:BC:32:D6:1D:43	100.4(12층 서브실)	Apple MacBook Pro	P)	2018-03-29 17:41:55	MACBOOKPRO-1D43	Apple, Inc.	
	동작	100%	진	2018-04-03 10:24:19			172.29.50.234	AC:BC:32:D6:1D:43	50.0 연구소IP대역	Apple MacBook Pro	P)		MACBOOKPRO-1D43	Apple, Inc.	
	동작	97%	진	2018-02-06 08:39:42	HP-2920-24G	1	172.29.59.201	8C:89:A5:E2:19:7A	59.0 (이민상팀장)	Microsoft Windows 10 Professional x64	P)		YSJIN-WIN10	Micro-Star INTL CO., LTD	
	동작	100%	조	2018-04-05 11:58:42	172.29.50.6	1	172.29.50.200	80:EA:96:E0:05:D6	50.0 연구소IP대역	Apple Device	P)	2018-04-05 11:34:33	jomyeongjin	Apple, Inc.	
	동작	41%	정	2018-04-03 09:06:11			172.29.20.90	1C:1B:0D:4F:35:34	S-172.29.20.4	Microsoft Windows 10 Professional x64	P)		DESKTOP-ET619IN	GIGA-BYTE TECHNOLOGY CO.,LTD.	
	동작	23%	정	2018-04-02 08:58:20			172.29.20.68	E0:D5:5E:59:BA:94	S-172.29.20.4	Microsoft Windows 10 Enterprise x64	P)		DESKTOP-E125H95	GIGA-BYTE TECHNOLOGY CO.,LTD.	
	동작	24%	정	2018-04-02 09:30:14			172.29.20.204	40:8D:5C:CF:C8:4F	S-172.29.20.4	Microsoft Windows 7 Professional x64	P)		COM-PC	GIGA-BYTE TECHNOLOGY CO.,LTD.	
	동작	85%	정	2018-04-02 17:30:21			172.29.20.20	FC:AA:14:AE:ED:D2	S-172.29.20.4	Microsoft Windows 7 Home x64	P)		A-PC	GIGA-BYTE TECHNOLOGY CO.,LTD.	
	동작	100%	장	2018-04-03 10:33:47			172.29.50.176	B8:E8:56:04:B6:B0	50.0 연구소IP대역	Apple MacBook Air	P)	2018-04-05 14:24:04	MACBOOKAIR-B6B0	Apple, Inc.	
	동작	11%	장	2018-04-03 10:33:47			172.29.60.55	B8:E8:56:04:B6:B0	60.0 (AGENT팀)	Apple MacBook Air	P)	2018-04-05 10:22:48	MACBOOKAIR-B6B0	Apple, Inc.	
	동작	100%	장	2018-04-02 09:55:43			172.29.50.160	00:0C:29:50:66:BC	50.0 연구소IP대역	Microsoft Windows 10 Professional x64	P)		DESKTOP-31UAUFT	VMware, Inc.	
	동작	19%	장	2018-04-05 11:33:23	172.29.50.6	1	172.29.50.197	AC:0D:1B:D5:1F:C4	50.0 연구소IP대역	LG Android Device	P)		android-898795b18a1e896	LG Electronics (Mobile Communications)	
	동작	85%	영	2018-02-19 07:54:35			172.29.50.239	40:8D:5C:79:FD:85	50.0 연구소IP대역	Microsoft Windows 10 Home x64	P)		WISEMANLIM-GENI	GIGA-BYTE TECHNOLOGY CO.,LTD.	
	동작	15%	이	2018-04-05 10:27:41			172.29.50.218	68:07:15:A2:27:3B	50.0 연구소IP대역	Microsoft Windows 10 Home x64	P)	2018-04-05 10:57:21	DESKTOP-YIHO25	Intel Corporate	
	동작	15%	이	2018-04-02 08:19:56			172.29.118.75	F4:8E:38:EC:3C:DE	118.0(이동희 선임)	Microsoft Windows 10 Home x64	P)	2018-04-05 10:56:51	DESKTOP-YIHO25	Dell Inc.	

## - 가시성 (2/3)

- 단말 내 다양한 정보 제공

**장비정보**

장비명: MS1 노트북 | 장비 ID: 39431f1c-c21b-1037-4001-d6bba8469c1

장비 설명: 전설형 업무용 노트북

**장비 세부 관리**

제조일: 2018-01-03 | 구매택: 구매센터서 등록 구매

대용량수 시작일: 2018-03-01 | 대용량수 만료일: 2021-03-01

일련번호: 123456789 | 구입가격: 1,200,000

책임자: 김관민 | 책임부서: 구매부

**네트워크정보**

장비내 IP: 172.29.112.56 | MAC: DE-CB:8A:34:D9:C1 | 포트명: FORE-ST-126 | 운영체제: Microsoft Windows 10 Professional x64

**이력관리**

시간	로그종류	로그ID	관리장비명	IP	MAC	사용자ID	사용자명	부서명	설명
2018-03-30 16:33:39	일일	시스템정보	172.29.112.100	172.29.112.56	D8:CB:8A:34:D9:C1				모니터 정보 추가 감지됨. SERIALNUMBER=000000000000
2018-03-30 16:33:31	일일	에이전트러션	172.29.112.100	172.29.112.56	D8:CB:8A:34:D9:C1				에이전트러션 결과. RESULT=ACTION=백신프로그램 종료. TYPE=NEW
2018-03-30 10:37:23	일일	설정변경	172.29.112.100	172.29.112.56	D8:CB:8A:34:D9:C1				장비의 속성이 변경됨. ADMIN=forest. ADMIN_IP=172.29.112.56
2018-03-30 10:01:23	일일	시스템정보	172.29.112.100	172.29.112.56	D8:CB:8A:34:D9:C1				모니터 정보 추가 감지됨. SERIALNUMBER=000000000000
2018-03-30 10:01:23	일일	시스템정보	172.29.112.100	172.29.112.56	D8:CB:8A:34:D9:C1				소프트웨어 목록 추가 감지됨. NAME=Droptop. VERSION=46.4.65. PATH=C:\Pro
2018-03-30 10:01:23	일일	시스템정보	172.29.112.100	172.29.112.56	D8:CB:8A:34:D9:C1				소프트웨어 목록 삭제 감지됨. NAME=Droptop. VERSION=45.4.92. PATH=C:\Pro
2018-03-29 09:42:50	일일	설정변경	172.29.112.100	172.29.112.56	D8:CB:8A:34:D9:C1				장비의 속성이 변경됨. ADMIN=forest. ADMIN_IP=172.29.112.56
2018-03-29 08:50:56	일일	시스템정보	172.29.112.100	172.29.112.56	D8:CB:8A:34:D9:C1				모니터 정보 추가 감지됨. SERIALNUMBER=unknown serial [BOE05E]
2018-03-29 08:50:56	일일	시스템정보	172.29.112.100	172.29.112.56	D8:CB:8A:34:D9:C1				모니터 정보 추가 감지됨. SERIALNUMBER=000000000000
2018-03-29 08:50:56	일일	시스템정보	172.29.112.100	172.29.112.56	D8:CB:8A:34:D9:C1				프린터 정보 추가 감지됨. PRINTERNAME=1172.29.100.160/Canon MB2300 ser
2018-03-29 08:50:56	일일	시스템정보	172.29.112.100	172.29.112.56	D8:CB:8A:34:D9:C1				프린터 정보 추가 감지됨. PRINTERNAME=(12)Canon IR-ADV C5030/C5035 C
2018-03-29 08:50:56	일일	시스템정보	172.29.112.100	172.29.112.56	D8:CB:8A:34:D9:C1				프린터 정보 추가 감지됨. PRINTERNAME=8종 캐논복합기

**시스템정보**

이전정보: Micro-Star International Co., Ltd | CPU: Intel(R) Core(TM) i7-4720HQ CPU @ 2.60GHz | CPU 제조사: Intel Corporation | 시분: 198339

메모리 정보: 전체: 15.82 GB | 사용: 2.86 GB | % 사용: 18%

저장장치 정보:

장치명	용량	변기명/파일명	고용번호	파일시스템	총 용량	사용된 용량	% 사용
C:	고용도라이브	/ TOSHIBA THNSJZ56G8JN	15G510GVTFMY	NTFS	227.28 GB	209.21 GB	92%
D: (차로디스크)	고용도라이브	/ LITEON CV1-48128	002543120266	NTFS	119.24 GB	71.01 GB	60%
E: (DimerCD)	고용도라이브	/ TOSHIBA THNSJZ56G8JN	15G510GVTFMY	NTFS	18 GB	9.38 GB	52%

운영체제 정보: Microsoft Windows 10 Professional x64 | 버전: 19.0.16299 | 서비스팩: 11.309.16299.0 | 언어: Korean | 사용자: zmond

인증정보: 도메인: FOREST-126 | WORKGROUP | 제품 Key: 2017-10-18 11:53:31 | 유효기간: 6 월, 22 시간, 57 분 | 자동 업데이트: 사용안함 | 액티브 디렉토리: 사용됨 | 원격 데스크톱: 허용안함

**소프트웨어정보**

백신 정보: Windows Defender | 제품 버전: 정보 없음 | 현재재판 버전: 1.263.1913.0 | 현재재판 날짜: 2018-04-02 05:55:37 | 실시간 검사: 중지

소프트웨어 정보:

프로그램명	버전	경로	설치일자	종료시간
Adobe Acrobat Reader DC - Korean	18.011.20038	C:\Program Files (x86)\Adobe\Acrobat Reader DC\	20180326	2018-03-29 08:50:44
Adobe Creative Cloud	4.4.1.298	C:\Program Files (x86)\Adobe\Creative Cloud\		2018-03-29 08:50:44
Adobe Premiere Pro CC 2017	11.1.2	C:\Program Files\Adobe		2018-03-29 08:50:44
Advanced ZIP Password Recovery (remove only)				2018-03-29 08:50:44
AhnLab Online Security		C:\Program Files (x86)\AhnLab\ASP\Common		2018-03-29 08:50:44
AhnLab Safe Transaction	1.3.26.1015	C:\Program Files\AhnLab\Safe Transaction	20180125	2018-03-29 08:50:44
AnySignalPC 1.1.0.11	1.1.0.11			2018-03-29 08:50:44
Apple Software Update	2.2.0.150	C:\Program Files (x86)\Apple Software Update	20171011	2018-03-29 08:50:44
AquaPlayer	1.9.17.0			2018-03-29 08:50:44
BitTorrent	7.10.0.43917	C:\Users\zmond\AppData\Roaming\BitTorrent		2018-03-29 08:50:44
Canon MB2300 series MP Drivers	1.04			2018-03-29 08:50:44
Chrome	65.0.3325.181	C:\Program Files (x86)\Google\Chrome\Application	20170101	2018-03-29 08:50:44
Cisco Spark	2.0.7753.0		20180321	2018-03-29 08:50:44
Cisco WebEx Meetings				2018-03-29 08:50:44
Deflino Q3 (x86) 버전 3.3.1.5	3.3.1.5	C:\Program Files (x86)\Wzvernal\Deflino-Q3\	20170525	2018-03-29 08:50:44
DirectCloud-BOX	1.0.43.0	C:\Users\zmond\AppData\Local\DirectCloud-BOX		2018-03-29 08:50:44
Droptop	46.4.65	C:\Program Files (x86)\Droptop\Client		2018-03-30 10:01:23
ESP 2.0	2.01			2018-03-29 08:50:44

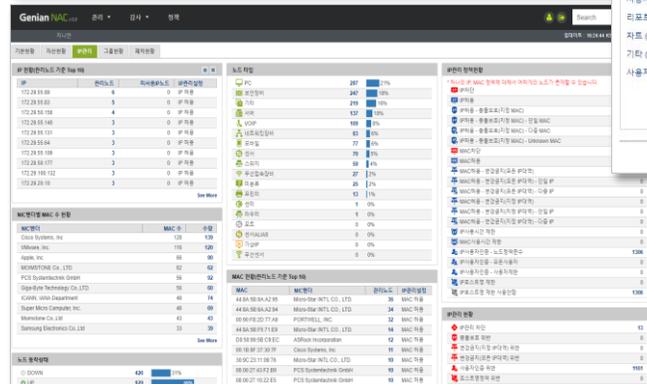
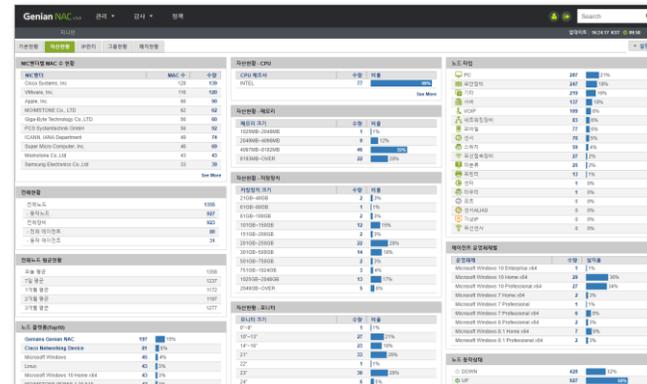
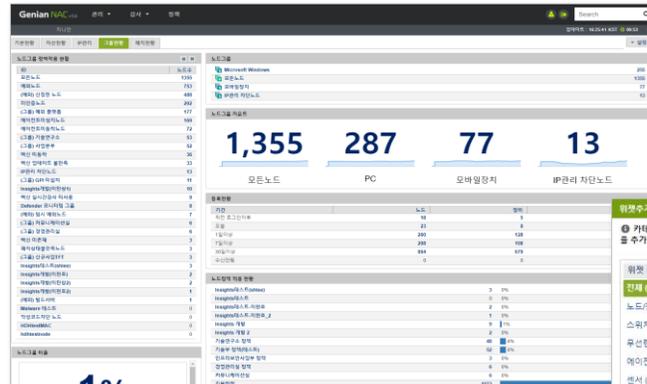
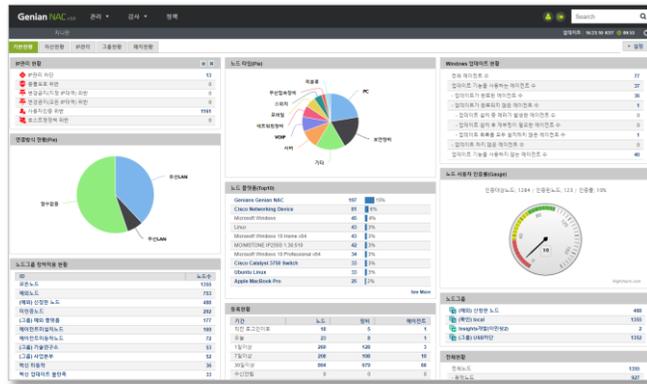
**운영체제 업데이트 정보**

업데이트명	분류	일시	업데이트 상태	설치유연상태	업데이트일자
2018-03-x64 기반 시스템용 Windows 10 Version 1709의 Adobe Flash Player 보안 업데이트(KB4088785)	보안 업데이트	2018-03-13	완료	미승인	2018-03-29 10:27:06
2018-03-x64 기반 시스템용 Windows 10 Version 1709에 대한 누적 업데이트(KB4088776)	보안 업데이트	2018-03-13	완료	미승인	2018-03-29 10:27:06
Microsoft Word 2013용 보안 업데이트(KB4011699) 32비트 버전	보안 업데이트	2018-03-13	완료	미승인	2018-03-29 10:27:06
Microsoft Excel 2013용 보안 업데이트(KB4018291) 32비트 버전	보안 업데이트	2018-03-13	완료	미승인	2018-03-29 10:27:06
Windows 약함 소프트웨어 제거 도구 x64 - 2018년 3월(KB890808)	업데이트 종료	2018-03-13	완료	미승인	2018-03-29 10:27:06
Skype for Business 2015용 업데이트(KB4018290) 32비트 버전	중요 업데이트	2018-03-06	완료	미승인	2018-03-29 10:27:06
Microsoft Office 2013용 업데이트(KB4018297) 32비트 버전	중요 업데이트	2018-03-06	완료	미승인	2018-03-29 10:27:06
Microsoft Project 2013용 업데이트(KB4018292) 32비트 버전	중요 업데이트	2018-03-06	완료	미승인	2018-03-29 10:27:06
Microsoft Office 2013용 업데이트(KB3172471) 32비트 버전	중요 업데이트	2018-03-06	완료	미승인	2018-03-29 10:27:06
Microsoft Office 2013용 보안 업데이트(KB3172469) 32비트 버전	보안 업데이트	2018-03-13	완료	미승인	2018-03-29 10:27:06
Microsoft Outlook 2013용 보안 업데이트(KB4011697) 32비트 버전	보안 업데이트	2018-02-13	완료	미승인	2018-03-29 10:27:06
Microsoft PowerPoint 2013용 업데이트(KB4011676) 32비트 버전	중요 업데이트	2018-02-06	완료	미승인	2018-03-29 10:27:06

# Cloud NAC 제품 소개

## - 가시성 (3/3)

- Dashboard를 통한 다양한 통계, 상태 등의 현황 파악에 용이



**위젯 추가**

카테고리별로 검색된 위젯목록에서 대상 위젯을 선정된 후 '대시보드에 추가' 버튼을 클릭하여 위젯을 추가하시거나 바꿉니다.

위젯 카테고리	위젯	설명		
전체 (24)	IP 현황(관리노드 기준 Top 10)	관리노드 기준으로 Top 10의 IP 현황을 표시합니다.		
	스위치 (48)	IP관리 정책현황	IP관리 정책별 카운트 현황을 목록으로 표시합니다.	
스위치 (10)	무선랜 (17)	IP관리 현황	노드의 IP관리 정태별 카운트를 목록으로 표시합니다.	
	메이스트 (20)	리포트 (2)	MAC 현황(관리노드 기준 Top 10)	관리노드 기준으로 Top 10의 MAC 현황을 표시합니다.
사용자 (14)	리포트 (2)	자문 (25)	NIC별단별 MAC 수 현황	NIC별단별 MAC 수 총이해 표시합니다.
	기타 (5)	사용자정보 (8)		

[닫기]

# 03

## Cloud NAC 제품 소개

### - 분류 (1/2)

- 다양한 분류 조건 제공 (Dynamic Classification)
- 분류 조건을 기준으로 그룹으로 생성 가능

#### 그룹 조건 예시

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
노트타입 / 감지된 노트타입이 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
노트그룹 / 속하면 / Microsoft Windows
에이전트상태 / 설치상태 / 설치안됨
위험감지 / 노트에 감지된 위험이 / 감지되면
시스템 / Windows 방화벽 / 사용안함

#### 분류 조건

- IP/MAC
- 등록일자
- 노드타입
- HOSTNAME
- 시스템 정보
- Agent 상태
- Platform
- 백신정보
- 사용자 계정
- 열린 Port
- Update 정보
- SW 정보
- TAG
- 패스워드
- On/Off
- 구입가격

## - 분류 (2/2)

- Dashboard를 통한 다양한 통계, 상태 등의 현황 파악에 용이

The dashboard provides a comprehensive overview of network and security data. Key sections include:

- 에이전트 운영체제 언어별 (Agent OS Language):** Shows the distribution of agent languages, with Korean at 99% and English at 1%.
- 에이전트 운영체제별 (Agent OS Type):** Lists various Windows operating systems, such as Windows 10 Enterprise x64 (1%) and Windows 7 Professional (1%).
- 노드 타입 (Node Type):** Categorizes nodes into PC (288, 21%), 서버 (121, 9%), and others like 모바일 (73, 5%) and 센서 (70, 5%).
- 노드그룹 정책적용 현황 (Node Group Policy Application Status):** A table showing the number of nodes where specific policies are applied, such as '모든노드' (1381) and '에이전트미설치노드' (169).
- 노드그룹 정책미적용 (Node Group Policy Not Applied):** Lists nodes where policies are not applied, including 'local' (1381) and 'USB차단' (1379).
- IP관리 정책현황 (IP Management Policy Status):** A detailed view of IP-related policies, including IP ranges (8), IP usage (1323), and MAC management (955).
- 제어정책 적용 현황 (Policy Application Status):** Shows the status of various control policies, such as 'HDH\_netctrl\_test' (77%) and '디펜드 미동작 차단' (3%).
- 등록현황 (Registration Status):** A bar chart showing the number of nodes registered over time, categorized by device type (PC, 서버, 모바일, 센서).
- Windows 업데이트 현황 (Windows Update Status):** A bar chart showing the distribution of Windows update statuses across nodes, including '진짜' (blue), '완료' (black), '미완료' (green), '미설치' (orange), and '불가' (purple).
- 노드 태그 (Node Tags):** A list of tags applied to nodes, such as 'HDH테스트' (0%), 'THREAT' (0%), and '고위험' (1%).

# 03

## Cloud NAC 제품 소개

### - 통제

- 차단, 알림의 통제 방법 제공

#### 차단 (Block)

- 

**조건에 따른 네트워크 차단**  
(신규 IP/MAC, 미 인증, 보안설정 위반 등)
- 

**특정 프로세스 중지(kill)**  
(관리자가 지정한 프로세스)
- 

**USB 장치 차단**  
(USB 저장장치 등 강제 off)

#### 알림 (Alarm)

- 

**사용자에게 알림**  
(차단 웹, agent 팝업, 인스턴스 메시지)
- 

**관리자에게 알림**  
(특정 이벤트 발생 시 SMS, E-mail 발송)
- 

**특정 로그 외부 전송**  
(타 보안 솔루션으로 로그 전송하여 모니터링)

#### 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 유도, 화면보호기 강제 설정 등)

## - 리포트 (1/2)

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

The screenshot displays the Genian NAC v5.0 interface. On the left, there is a sidebar with navigation options like '로그' (Log), '로그검색' (Log Search), and '검색' (Search). The main area shows a log report for the week of 2018-03-26 to 2018-04-02. A bar chart at the top of the report shows log volume over time. Below the chart is a table of log entries with columns for '시간' (Time), '로그종류' (Log Type), '로그ID' (Log ID), '관리장비명' (Device Name), 'IP', 'MAC', '사용자ID' (User ID), '사용자명' (User Name), and '부서명' (Department Name). Several entries are highlighted in yellow, indicating warnings or errors.

Overlaid on the screenshot are several informational boxes:

- Boolean Operators:** Boolean operators (논리 연산자)는 용어들이 logic 연산자를 통해 결합될 수 있도록 합니다. AND, "+", OR, NOT 그리고 "-" 과 같은 Boolean operators(논리 연산자)를 지원합니다.
- Wildcard Searches:** wildcard 검색을 위해 단독 그리고 다양한 문자를 지원합니다. 단독 문자 wildcard 검색을 실행하기 위해 "?"를 사용합니다. 다양한 문자 wildcard 검색을 실행하기 위해 "\*"를 사용합니다.
- Fuzzy Searches:** fuzzy 검색을 지원합니다. Fuzzy 검색을 위해 hide를 사용합니다. 단독 단어의 끝에 ~ 표시하십시오. 예를 들어, "roam"과 스펠링이 유사한 단어를 검색하기 위해 fuzzy 검색을 사용합니다.
- 현재 검색조건을 검색기간 (1주) 으로 검색필터에 저장합니다.**
- 검색필터:**  검색필터를 로그 트리 및 로그모니터에 표시합니다.
- 출력설정:** A table with columns '사용가능' (Available) and '선택' (Selected). The '시간' (Time) and '로그종류' (Log Type) columns are selected.
- 알림전송:**  해당 로그 발생시 관리자에게 알림을 전송합니다.
- SYSLLOG 전송:**  해당 로그 발생시 SYSLOG서버로 전송합니다.
- SNMP Trap 전송:**  해당 로그 발생시 SNMP서버로 SNMP Trap을 전송합니다.
- Webhook:**  해당 로그 발생시 설정한 URL레이저를 호출합니다.
- 태그:** NONE

## - 리포트 (2/2)

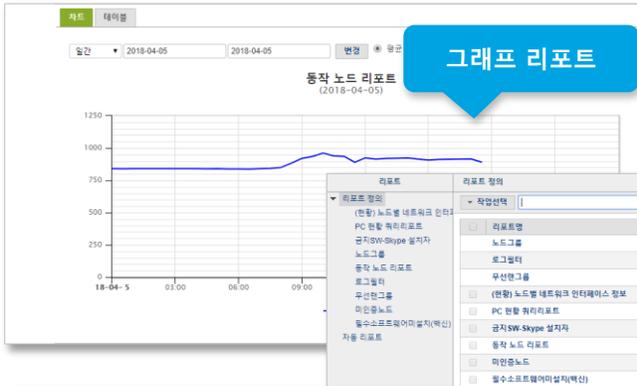
- 노드, 쿼리, 로그 리포트 제공

이름	이동률				변동폭		
	오늘	전일	전주	전월	전일비	전주비	전월비
에이전트등록노드	55	109	107	93	▲54	▼52	▼38
동작노드	891	843	865	735	▲48	▲26	▲156
예외노드	722	752	730	656	▼30	▼8	▲66
컴플라이언스 위반노드	473	496	490	426	▼23	▼17	▲47
위험감지노드	423	408	398	347	▲15	▲25	▲76
(예외) 신장한 노드	457	444	496	424	▲13	▼39	▲33
(그룹) USB저장	1373	1361	1362	1190	▲12	▲11	▲183
(확인) local	1375	1363	1364	1192	▲12	▲11	▲183
모든노드	1375	1363	1364	1192	▲12	▲11	▲183
(그룹) 예외 플랫폼	158	166	180	140	▼8	▼22	▲18
모바일장치	70	78	76	70	▼8	▼6	0
패치상태불만족노드	8	3	2	21	▲5	▲6	▼13
(그룹) 기술연구소	45	49	49	27	▼4	▼4	▲18
미인증노드	1	1	1	1	▼4	▼2	▼7
(그룹) 사업본부	1	1	1	1	▼5	▼2	▼1
백신 실시간검사 사용	1	1	1	1	▼5	▼2	▼3
화면보호기 미설정	5	5	5	0	▼2	▼2	▲3
(그룹) 해외사업부	2	1	1	2	▲1	▲1	▲1
(예외) 빌드서버	2	1	1	1	▲1	▲1	▲1
Apple Mac OS	37	38	37	38	▼1	0	▼1
insights개발(0, '1)	10	11	10	10	▼1	0	0

증감 추이 리포트

IP	MAC	인증사용자	부서	관리센터	CPU	전체메모리	사용메모리	메모리사용률
172.158.4.70	B8:EE:5B:33	최	전략사업부	S-172	158 Intel(R) Core(TM) i3-3220 CPU @ 2.40GHz	821872	2019740	24%
172.78.00	E0:4C:36:06:99	환	전략사업부	S-172	78 Intel(R) Core(TM) i5-4210U CPU @ 1.70GHz	8294176	2094956	25%
172.228.08	34:89:AE:C9	환	NAC 개발실	S-172	228 Intel(R) Core(TM) i3-3337U CPU @ 1.80GHz	8091952	1843548	23%
172.229.02	EA:12:1C:08:0B	환	신규사업FFT	S-172	229 Intel(R) Core(TM) i7-4700K CPU @ 4.00GHz	16446028	1441332	9%
172.219.80	E8:50:9F:50:88							
172.41.00	D7:88:D9:3C:8E				41 Intel(R) Core(TM) i3-3220 CPU @ 2.40GHz	3649584	1677780	46%
172.42.00	E0:4C:39:48:43				42 Intel(R) Core(TM) i5-4210U CPU @ 1.70GHz	8294176	2094956	25%
172.58.00	50:99:91:D3:70				58 Intel(R) Core(TM) i7-4700K CPU @ 4.00GHz	16446028	1441332	9%
172.189.00	28:20:89:DA:28							
172.161.00	E0:4C:69:01:11	최	기술연구소	S-172	161 Intel(R) Core(TM) i3-3220 CPU @ 2.40GHz	821872	2019740	24%
172.129.04	B8:76:77:AA:06	환	Endpoint 개발실	S-172	129 Intel(R) Core(TM) i5-3337U CPU @ 1.80GHz	8091952	1843548	23%
172.180.40	8D:5C:70:7F:22	환	Endpoint 개발실	S-172	180 Intel(R) Core(TM) i7-4700 CPU @ 4.00GHz	1663244	13101372	61%
172.199.6C	4D:73:DA:29:09	환	Insights 개발실	S-172	199 Intel(R) Core(TM) i3-3220 CPU @ 2.40GHz	821872	2019740	24%
172.234.0C	BC:32:D6:1D:43	환	Insights 개발실	S-172	234 Intel(R) Core(TM) i3-3220 CPU @ 2.40GHz	821872	2019740	24%
172.201.8C	89:AS:E2:19:7A	환	Insights 개발실	S-172	201 Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz	16708188	13099796	78%
172.200.80	EA:98:E0:05:06	환	NAC 개발실	S-172	200 Intel(R) Core(TM) i3-3220 CPU @ 2.40GHz	821872	2019740	24%
172.90.1C	18:0D:4F:35:34	환	감정관리실	S-172	90 Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz	16687544	3994992	24%
172.88.00	E5:DE:59:BA:94	환	감정관리실	S-172	88 Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz	16687544	3994992	24%
172.204.00	AA:5C:CF:C8:4F	환	감정관리실	S-172	204 Intel(R) Core(TM) i7-4700K CPU @ 4.00GHz	16554776	3126368	19%
172.20.00	FC:AA:14:AE:ED:02	환	감정관리실	S-172	20 Intel(R) Core(TM) i3-4160 CPU @ 3.60GHz	1665258	6833784	41%

쿼리 리포트 (관리자 지정)



리포트 현황

과일명	생성일자
(현황) 노드별 네트워크 인터페이스 정보-180405-100001454.xls	2018-04-05 10:00:01
(현황) 노드별 네트워크 인터페이스 정보-180330-100001186.xls	2018-04-04 10:00:01
(현황) 노드별 네트워크 인터페이스 정보-180329-100001149.xls	2018-04-03 10:00:01
(현황) 노드별 네트워크 인터페이스 정보-180328-100001450.xls	2018-04-02 10:00:01
(현황) 노드별 네트워크 인터페이스 정보-180401-100001122.xls	2018-04-01 10:00:01
(현황) 노드별 네트워크 인터페이스 정보-180331-100001183.xls	2018-04-01 10:00:01
(현황) 노드별 네트워크 인터페이스 정보-180327-100007628.xls	2018-03-27 10:00:01
(현황) 노드별 네트워크 인터페이스 정보-180323-100000903.xls	2018-03-23 10:00:01
(현황) 노드별 네트워크 인터페이스 정보-180322-100001403.xls	2018-03-22 10:00:01
(현황) 노드별 네트워크 인터페이스 정보-180322-100001268.xls	2018-03-22 10:00:01
(현황) 노드별 네트워크 인터페이스 정보-180321-100001563.xls	2018-03-21 10:00:01
(현황) 노드별 네트워크 인터페이스 정보-180320-100001308.xls	2018-03-20 10:00:01
(현황) 노드별 네트워크 인터페이스 정보-180319-100001187.xls	2018-03-19 10:00:01

스케줄 가능

엑셀 변환

cnt	NI_DEVID	MAC	ADDR	NI_NETMASK
2	0e8b6072-8028-1036-8018-448a627093f	Wi-Fi	172.158.4.70	255.255.255.0
2	0e8b6072-8028-1036-8018-448a627093f	이더넷	172.158.4.70	255.255.255.0
4	0e9fcc48-8536-1037-8194-00e04c504624	10 Ethernet adapter	172.28.50.167	255.255.255.0
4	0e9fcc48-8536-1037-8194-00e04c504624	Wi-Fi	172.28.50.167	255.255.255.0
4	0e9fcc48-8536-1037-8194-00e04c504624	이더넷 2	172.28.50.167	255.255.255.0
4	0e9fcc48-8536-1037-8194-00e04c504624	이더넷 7	172.28.50.167	255.255.255.0
2	0003306a-821e-1001-8002-000ec0f0b03	Wi-Fi	196.255.255.255	255.255.255.0
2	0003306a-821e-1001-8002-000ec0f0b03	이더넷 2	196.255.255.255	255.255.255.0
3	1337fa98-98cc-1036-8064-184a7f7038a2	포털 원격 연결	172.158.4.70	255.255.255.0
3	1337fa98-98cc-1036-8064-184a7f7038a2	포털 원격 연결 2	172.158.4.70	255.255.255.0
3	1337fa98-98cc-1036-8064-184a7f7038a2	공인 네트워크 연결	172.158.4.70	255.255.255.0
4	18130384-8353-1036-803a-48805c798885	WPA_VPN Client	172.158.4.70	255.255.255.0
4	18130384-8353-1036-803a-48805c798885	이더넷 4	172.158.4.70	255.255.255.0
4	18130384-8353-1036-803a-48805c798885	이더넷 4	172.158.4.70	255.255.255.0
3	1856abc-2551-1037-8364-18678cc0c020	Wi-Fi	172.158.4.70	255.255.255.0
3	1856abc-2551-1037-8364-18678cc0c020	이더넷	172.158.4.70	255.255.255.0
4	20c8b094-04a4-1037-807a-98839145191	이더넷 2	172.158.4.70	255.255.255.0
4	20c8b094-04a4-1037-807a-98839145191	이더넷 2	172.158.4.70	255.255.255.0
4	20c8b094-04a4-1037-807a-98839145191	이더넷 3	172.158.4.70	255.255.255.0
2	209619e-8ee8-1037-8274-0a2917022631	Wi-Fi	172.158.4.70	255.255.255.0
2	209619e-8ee8-1037-8274-0a2917022631	이더넷 8	172.158.4.70	255.255.255.0
2	20a6a48-844c-1036-8051-00e04c504624	Wi-Fi	172.158.4.70	255.255.255.0
2	20a6a48-844c-1036-8051-00e04c504624	이더넷	172.158.4.70	255.255.255.0
3	3546a828-9718-1036-8050-00b2a6c78	Wi-Fi	172.158.4.70	255.255.255.0
3	3546a828-9718-1036-8050-00b2a6c78	이더넷	172.158.4.70	255.255.255.0
3	3546a828-9718-1036-8050-00b2a6c78	이더넷 2	172.158.4.70	255.255.255.0
2	35e8a766-3761-1037-8141-98839145191	Wi-Fi	172.158.4.70	255.255.255.0
2	35e8a766-3761-1037-8141-98839145191	이더넷	172.158.4.70	255.255.255.0
3	367c786-8376-1036-8037-18678cc0c020	Wi-Fi	172.158.4.70	255.255.255.0
3	367c786-8376-1036-8037-18678cc0c020	포털 원격 연결 *4	172.158.4.70	255.255.255.0
3	367c786-8376-1036-8037-18678cc0c020	이더넷	172.158.4.70	255.255.255.0
3	382a292c-2468-1037-8012-18678431360	Wi-Fi	172.158.4.70	255.255.255.0

## - Cloud NAC 기능 요약

- 다양한 방식의 접근 제어 가능

### Agent-less

<b>Platform 분류</b>	OS(Win, Linux, Unix, iOS, Android 등)별, 네트워크 장비, 프린터, 제조사 등
<b>접근제어</b>	IP, MAC, PORT, Protocol 별 접근제어
	Platform 별 접근 제어(OS 및 장치 별)
	시간/요일/기간 접근 제어
	사용자 별 접근제어(인증/미 인증, ID, 부서, 직급 등)
<b>네트워크 정보</b>	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 없는 환경에서도 다양한 방식으로 접근제어

### Agent

<b>MSOS, Office 패치</b>	Windows patch, MS office patch
<b>시스템 정보</b>	PC H/W 정보(CPU, MEM, DISK, OS, NIC 등), Hostname 수집 및 제어
<b>세션 제어</b>	TCP 세션 정보 수집 및 임계치 초과시 차단
<b>포트 정보</b>	열린 포트, 포트 사용 프로세스, 서비스 정보
<b>장치제어</b>	USB, NIC, Bluetooth, Wifi, Tethering, PC전원 제어
<b>프로세스 제어</b>	특정 프로세스 강제 중지
<b>백신 연동</b>	백신(v3, 바이로봇, 알약)업데이트 및 바이러스 탐지에 대한 네트워크 제어
<b>소프트웨어 탐지</b>	필수 S/W, 불법 S/W 탐지 및 제어
<b>메시지 전송</b>	사용자에게 메시지 전송(공지 및 알림 팝업)
<b>보안기능</b>	비번 유효성 검사, 윈도우 보안 설정, 자동 실행 제어, 파일 배포, 공유 폴더 제어, 화면보호기 제어, IE 보안 설정 제어, 윈도우 방화벽 제어, 계정 취약성 검사, 공유폴더 제어
<b>위 변조 탐지</b>	IP, MAC clone 탐지/차단
<b>AP탐지</b>	무선 AP 탐지 및 접속 제어
<b>시스템 정보</b>	OS, H/W 정보(CPU, MEM, DISK, OS, NIC 등)
<b>소프트웨어 탐지</b>	설치된 프로그램 정보확인, 백신 정보 확인
<b>OS 패치</b>	MAC OS 업데이트



## - Cloud NAC 제품 특징점

- 다양한 DB와 연동을 통해 NAC에 특정 정보 자동 등록/관리 가능

ORACLE  
MYSQL  
MSSQL/Sybase  
IBM DB2  
Tibero  
Altibase  
PostgreSQL  
LDAP  
CSV  
CSV(Upload)  
CUBRID

**노드정보**

노드정보데이터명

노드정보조건문

IP주소결함명

MAC주소결함명

노드이름결함명

노드설명결함명

인증사용자ID결함명

추가정보1결함명

추가정보2결함명

추가정보3결함명

**사용자정보**

사용자데이터명

사용자조건문

사용자ID결함명

사용자이름결함명

패스워드결함명

원본 암호와 알고리즘

변경시각 결함명

변경시각 비교결함명

패스워드암호화알고리즘결함명

회사이름결함명

부서ID결함명

직급ID결함명

전화번호결함명

휴대폰결함명

이메일결함명

주소결함명

설명결함명

추가정보1결함명

추가정보2결함명

추가정보3결함명

NTAG 85	위험	동작	IP주소	MAC주소	정책	제어정책	호스트(이름)	플랫폼	인증사용자	위치	기능률
172.29.112.4	0	0	44.5A.5B.8A.A2.95		기본정책					\$-172.29.112.100	99%
172.29.112.49	0	0	00.90.FB.20.77.A9		기본정책		Genians Genians NAC			\$-172.29.112.100	100%
172.29.112.50	0	0	84.E5.99.07.78.C9		기본정책		EPM Networks upTIME			\$-172.29.112.100	100%
172.29.112.58	0	0	08.CB.84.CD.C1		기본정책		FOREST-USB			\$-172.29.112.100	20%
172.29.112.59	0	0	AC.E0.10.81.A1.9F		기본정책		Microsoft Windows			\$-172.29.112.100	2%
172.29.112.67	0	0	80.F9.1D.8E.AA.30		기본정책		MACBOOKPRO-A880			\$-172.29.112.100	7%
172.29.112.69	0	0	E4.F4.ED.1C.20.27		기본정책		Samsung-GALAXY-S7			\$-172.29.112.100	2%
172.29.112.73	0	0	8B.CA.68.3C.CF.3E		기본정책		Dangguu-iPhone			\$-172.29.112.100	2%
172.29.112.75	0	0	09.33.11.04.F9.DE		기본정책		Apple iPhone			\$-172.29.112.100	53%
172.29.112.80	0	0	AC.E0.10.81.A1.9F		기본정책		일건용			\$-172.29.112.100	0%
172.29.112.80	0	0	AA.AA.AA.CC.CC.CC		기본정책		일건용			\$-172.29.112.100	21%

**장비수명주기정보**

제조일

내용연수 시작일

구입처

구입가격

책임자

책임부서

내용연수 만료일

메모

추가정보1결함명

추가정보2결함명

추가정보3결함명

추가정보

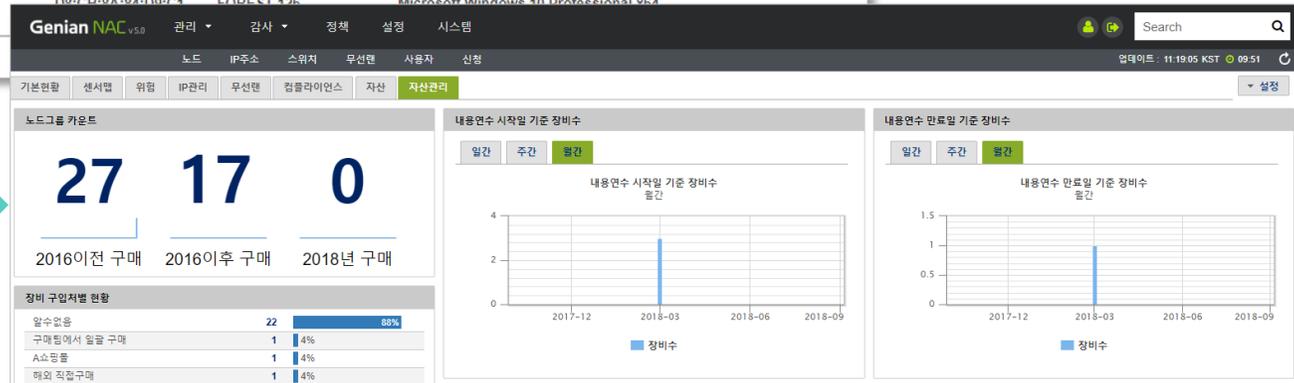
## - Cloud NAC 제품 특징점

- 장비 수명주기 관리 기능 제공

기본정보	장비정보	시스템정보	네트워크정보	소프트웨어정보	운영체제 업데이트 정보	이력관리	IP관리	정책	정책현황
장비명	MSI 노트북	장비 ID	39a3f1ce-c28b-1037-8001-d8cb8a84d9c1						
장비설명	컨설팅 업무용 노트북								
장비 수명주기 관리									
제조일	2016-01-02	구입처	구매팀에서 일괄 구매						
내용연수 시작일	2016-01-05	내용연수	3	년	내용연수 만료일	2019-01-05			
일련번호	123456789								
책임자	김관리	구입가격	1,200,000						
메모		책임부서	구매부						
장비내 노드	IP	MAC	호스트명	플랫폼					
	172.29.112.56	D8:CB:8A:84:D9:C4	FOREST-126	Microsoft Windows 10 Professional x64					

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

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



## - Cloud NAC 제품 특징점

- 플랫폼 자동 분류 기능 단말 플랫폼 인텔리전스 (DPI) 제공



SOLUTIONS ▾

GENIAN NAC ▾

RESOURCES ▾

COMPANY ▾



TRIAL &amp; BUY

Device Platform Intelligence / Cisco Catalyst 2960X-24TS-LL Switch



## Cisco Catalyst 2960X-24TS

Platform Information <http://www.router-switch.com/ws-c2960x->Search Engine [Search on Google](#)End of Sales Yes (2015-11-06) [more info](#)End of Support Planned (2020-11-30) [more info](#)

Wired Connection Yes

Wireless Connection -

Fingerprinting Source [NIC VENDOR](#) [SNMP OID](#)

Added at Aug 20, 2014

Manufacturer Name Cisco Systems Inc.

단말 및 제조사 취약점 정보  
(CVE No/Severity/Description)

Manufacturer's Common Vulnerabilities and Exposures (CVE)

CVE-ID	Severity v3.0	Severity v2.0	Description
CVE-2019-1841 04/18/2019	HIGH	MEDIUM	A vulnerability in the Software Image Management feature of Cisco DNA Center could allow an authenticated, remote attacker to access to internal services without additional authentication. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending arbitrary HTTP requests to internal services. An exploit could allow the attacker to bypass any firewall or other protections to access unauthorized internal services. DNAC versions prior to 1.2.5 are affected.
CVE-2019-1840 04/18/2019	HIGH	HIGH	A vulnerability in the DHCPv6 input packet processor of Cisco Prime Network Registrar could allow an unauthenticated, remote attacker to restart the server and cause a denial of service (DoS) condition on the affected system. The vulnerability is due to incomplete user-supplied input validation when a custom

## - Cloud NAC 제품 특징점

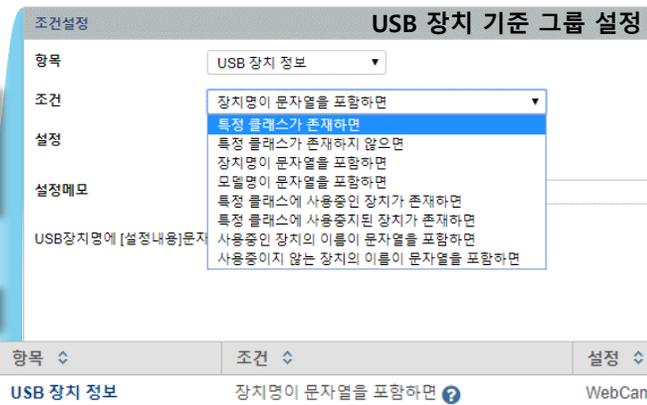
- USB 장치 정보 자동 수집 및 조건 설정 그룹 생성

## 장치정보



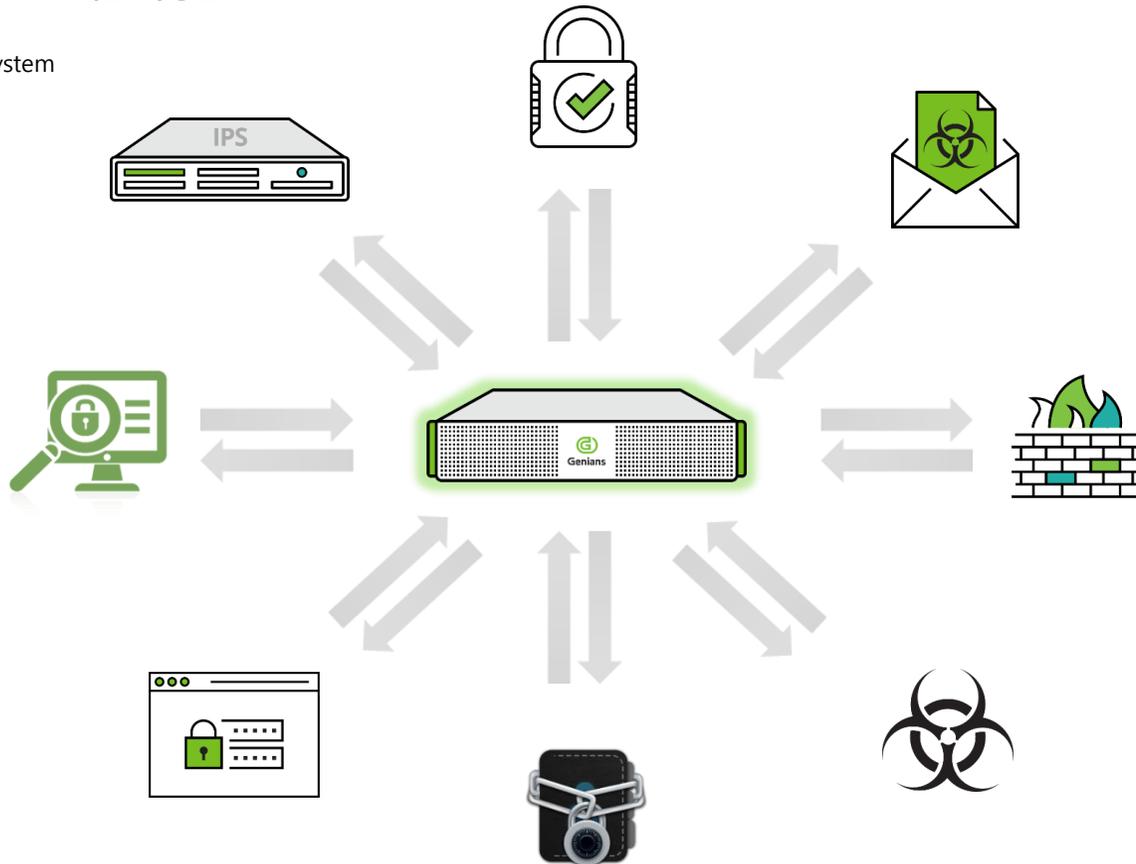
## NAC 에 등록된 USB 정보

USB 정보	장치명	제조사	모델명	시리얼	상태
Bluetooth	MX Anywhere 2				사용
Bluetooth	Microsoft Bluetooth 열거자				사용
Bluetooth	Microsoft Bluetooth 프로토콜 지원 드라이버				사용
네트워크 어댑터	Bluetooth Device (Personal Area Network)				사용중지
네트워크 어댑터	Bluetooth Device (RFCOMM Protocol TDI)				사용
키보드	HID 키보드 장치	Logitech	USB Receiver		사용
마우스 및 기타 포인팅 장치	HID 규격 마우스	Logitech	USB Receiver		사용
카메라	NEC HD WebCam			200901010001	사용
DriverInterface	Logitech Driver Interface	Logitech	USB Receiver		사용



## - Cloud NAC 제품 특징점

## - Security Ecosystem

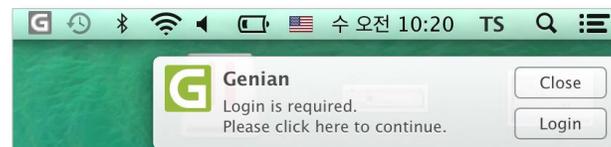
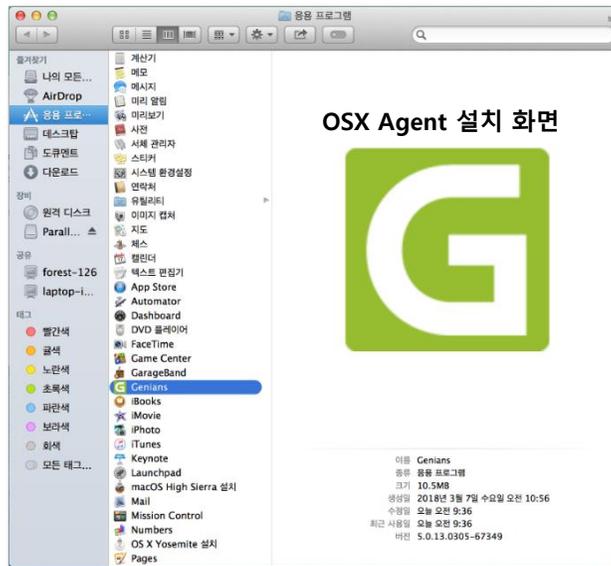


## 다양한 보안 시스템과의 연동 제공

1. Syslog
  - 송/수신 기능
  - 로그 수신 후 해당 IP 에 대한 제어
2. Snmptrap
  - 송/수신 기능
  - 로그 수신 후 해당 IP 에 대한 제어
3. Rest API
  - 타 그룹웨어와의 연동을 위한 유연한 방식
  - 신청/결재 시스템 연동
4. DB 연동
  - DB 연동으로 추가적인 정보 제공

## - Cloud NAC 제품 특징점

- MAC OS (OSX) Agent 지원



OSX 로그인 팝업

## OSX 노트 정보

<input type="checkbox"/>		<input type="checkbox"/>	172.29.112.60	AC:E0:10:61:A1:0F		기본정책	임	Microsoft Windows
<input type="checkbox"/>		<input type="checkbox"/>	172.29.112.61	80:E6:50:0F:5F:6C		기본정책	gunwoogui-macbook-pro.local	Apple OS X Mavericks
<input type="checkbox"/>		<input type="checkbox"/>	172.29.112.67	60:F8:1D:BE:AA:90		기본정책	MACBOOKPRO-AA90	Apple MacBook Pro

## OSX Agent 수집 정보

OS ↑	PT	액션명	플러그인명	설명
		운영체제정보 수집	운영체제정보 수집	macOS 운영체제 정보 및 사용자 정보를 수집하여 노트정보에 표시합니다.
		하드웨어정보 수집	하드웨어정보 수집	마더보드 정보, 메모리정보, 저장장치 정보를 수집하여 노트정보에 표시합니다.
		소프트웨어정보 수집	소프트웨어정보 수집	설치된 소프트웨어정보를 수집하여 노트정보의 [소프트웨어정보][소프트웨어목록]에 표시합니다.
		네트워크정보 수집	네트워크정보 수집	네트워크 인터페이스 정보를 수집하여 노트정보에 표시합니다.
		백신정보 수집	백신정보 수집	PC에 설치되어있는 백신프로그램 정보를 수집합니다.
		macOS 업데이트	macOS 업데이트	macOS의 업데이트 상태를 검사하고 설정에 따른 최신 업데이트를 수행합니다.

## Software 정보 수집

백신 정보

백신명	제품 버전
Apple OS X Mavericks	
Apple OS X El Capitan	
Apple macOS High Sierra	

소프트웨어 정보

프로그램명	버전	출처	경로	최근변경시간	등록된시간
AirPort 유틸리티	6.3.2	apple	/Applications/Utilities/AirPort Utility.app	5/22/13, 5:05 AM	2018-04-04 09:38:54
App Store	1.3	apple	/Applications/App Store.app	5/14/13, 2:01 AM	2018-04-04 09:38:54
Apple OS X Mavericks	10.9.5	apple	Macintosh HD		2018-04-04 09:38:54
AppleScript 편집기	2.6.1	apple	/Applications/Utilities/AppleScript Editor.app	4/25/13, 6:23 AM	2018-04-04 09:38:54
Automator	2.4	apple	/Applications/Automator.app	4/20/13, 2:15 AM	2018-04-04 09:38:54
Bluetooth 파일 교환	4.2.7	apple	/Applications/Utilities/Bluetooth File Exchange.app	2/13/18, 12:18 PM	2018-04-04 09:38:54
Boot Camp 지원	5.1.2	apple	/Library/Utilities/Boot Camp Assistant.app	3/21/14, 8:19 AM	2018-04-04 09:38:54
Cocoa-AppleScript Applet	1.0	unknown	/Library/Application Support/Script Editor/Templates/Cocoa-AppleScript Applet.app	1/15/14, 2:17 PM	2018-04-04 09:38:54
ColorSync 유틸리티	4.9.0	apple	/Applications/Utilities/ColorSync Utility.app	8/25/13, 2:57 PM	2018-04-04 09:38:54
Dashboard	1.8	apple	/Applications/Dashboard.app	8/25/13, 10:38 AM	2018-04-04 09:38:54
Droplet with Settable Properties	1.0	unknown	/Library/Application Support/Script Editor/Templates/Droplets/Droplet with Settable Properties.app	1/15/14, 2:17 PM	2018-04-04 09:38:54
DVD 플레이어	5.7	apple	/Applications/DVD Player.app	12/9/13, 2:44 PM	2018-04-04 09:38:54
FaceTime	3.0	apple	/Applications/FaceTime.app	5/16/14, 8:44 AM	2018-04-04 09:38:54
Feedback Assistant	unknown	unknown	/System/Library/CoreServices/Feedback Assistant.app	3/23/14, 4:56 AM	2018-04-04 09:38:54

OSX 지원 버전

전체

Apple OS X Mavericks

Apple OS X El Capitan

Apple macOS High Sierra

Apple OS X Yosemite

Apple macOS Sierra

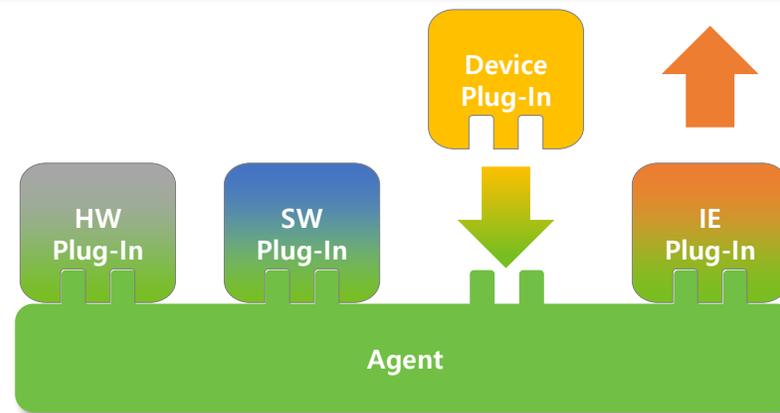
## - Cloud NAC 제품 특징점

- 사용자 PC의 안정성을 보장하는 Agent



- 모든 기능 플러그인 형태로 제공하여 선택/추가 용이함
- 선택적 기능 사용으로 리소스 사용 최소화
- Non-Kernel 기반의 동작(OS 충돌 위험 거의 없음)

OS	PT	역선명	플러그인명	설명
Windows	사용자	사용자 알림메시지	사용자 알림메시지	사용자에게 알림메시지를 표시합니다.
Windows	프로그램	프로그램 제거	프로그램 제거	제어판의 프로그램 제거에 등록된 프로그램중 제거 가능한 특정 프로그램을 제거합니다.
Windows	DNS	DNS 제어	DNS 제어	DNS 관련 로컬설정을 제어합니다.
Windows	유선랜	유선랜 인증 프로파일 설정	유선랜 인증 프로파일 설정	유선랜인터페이스의 802.1x 인증 프로파일 설정을 강제화 한다.
Windows	네트워크	네트워크 트래픽 제어	네트워크 트래픽 제어	주기적으로 네트워크 사용량을 수집하여 설정된 수치 이상일 경우 네트워크 인터페이스를 차단합니다.
macOS	운영체제	운영체제정보 수집	운영체제정보 수집	macOS 운영체제 정보 및 사용자 정보를 수집하여 노드정보에 표시합니다.
macOS	하드웨어	하드웨어정보 수집	하드웨어정보 수집	마더보드 정보, 메모리정보, 저장장치 정보를 수집하여 노드정보에 표시합니다.
macOS	소프트웨어	소프트웨어정보 수집	소프트웨어정보 수집	설치된 소프트웨어정보를 수집하여 노드정보의 [소프트웨어정보][소프트웨어목록]에 표시합니다.
macOS	네트워크	네트워크정보 수집	네트워크정보 수집	네트워크 인터페이스 정보를 수집하여 노드정보에 표시합니다.
macOS	백신	백신정보 수집	백신정보 수집	PC에 설치되어있는 백신프로그램 정보를 수집합니다.
macOS	업데이트	macOS 업데이트	macOS 업데이트	macOS의 업데이트 상태를 검사하고 설정에 따른 최신 업데이트를 수행합니다.



# 03

## Cloud NAC 제품 소개

- Cloud NAC 도입 후 네트워크 사용 절차 (1/2)

- 단계별 정책 준수 후 네트워크 허용 프로세스

### 최초 미 승인 단말



### IP관리 정책

신규 IP/MAC 차단  
 IP 변경금지 차단  
 미 사용 IP 삭제 후 재 사용 시 차단

### 인증 정책

최초 1회 인증  
 주기적 인증  
 외부직원 인증  
 임직원 인증

### Agent 정책

NAC Agent 미 설치 차단  
 필수 SW 미 설치 차단  
 OS 보안 취약 단말 차단/교정  
 패스워드 미 설정/공유폴터 사용

### 보안 정책 준수 후 네트워크 사용

# 03

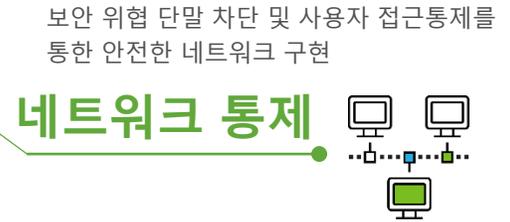
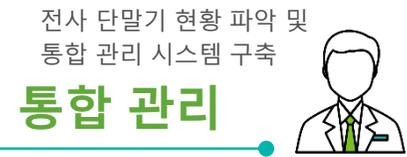
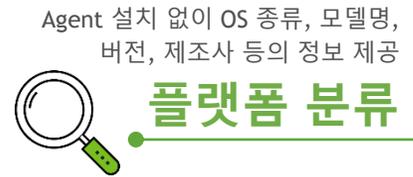
## Cloud NAC 제품 소개

### - Cloud NAC 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 인증을 통한 IP 실명제



The logo consists of several overlapping, semi-transparent circles in various shades of green and teal, creating a layered, organic shape. The text 'Genian NAC' is centered within this shape in white.

Genian  
NAC

---

## 회사 소개

---

## - NAC 기술 기반 보안 플랫폼 기업 지니언스!



## Genian NAC

## Genian NAC

BYOD 환경에서 유무선을 아우르는 내부 보안 관리 체계를 운영할 수 있는 '네트워크 접근제어(NAC : Network Access Control) 솔루션'

## Genian Insights E



## Genian Insights E

내부 네트워크와 단말에 대한 악성 행위를 파악하고 이상 징후를 빠르게 탐지할 수 있는 '빅데이터 엔진 기반 엔드포인트 위협탐지 및 대응 플랫폼'



## Genian GPI

## Genian GPI

PC의 보안 취약점을 점검하고 사용자가 스스로 조치할 수 있도록 행동 변화를 유도해 보안 체질을 개선할 수 있는 'PC 보안 수준 진단 솔루션'

## 회 사 명

(주)지니언스

## 대 표 이 사

이 동 범

## 설 립 일

2005년 01월 07일

## 자 본 금

20억

## 주 요 사 업

네트워크 보안 솔루션 개발/판매,  
보안감사(audit) 솔루션 개발/판매

## 임 직 원 수

139명 (20년 현재)

## 협 력 사

론스텍(총판), 대신정보통신(총판)등 약 30개사

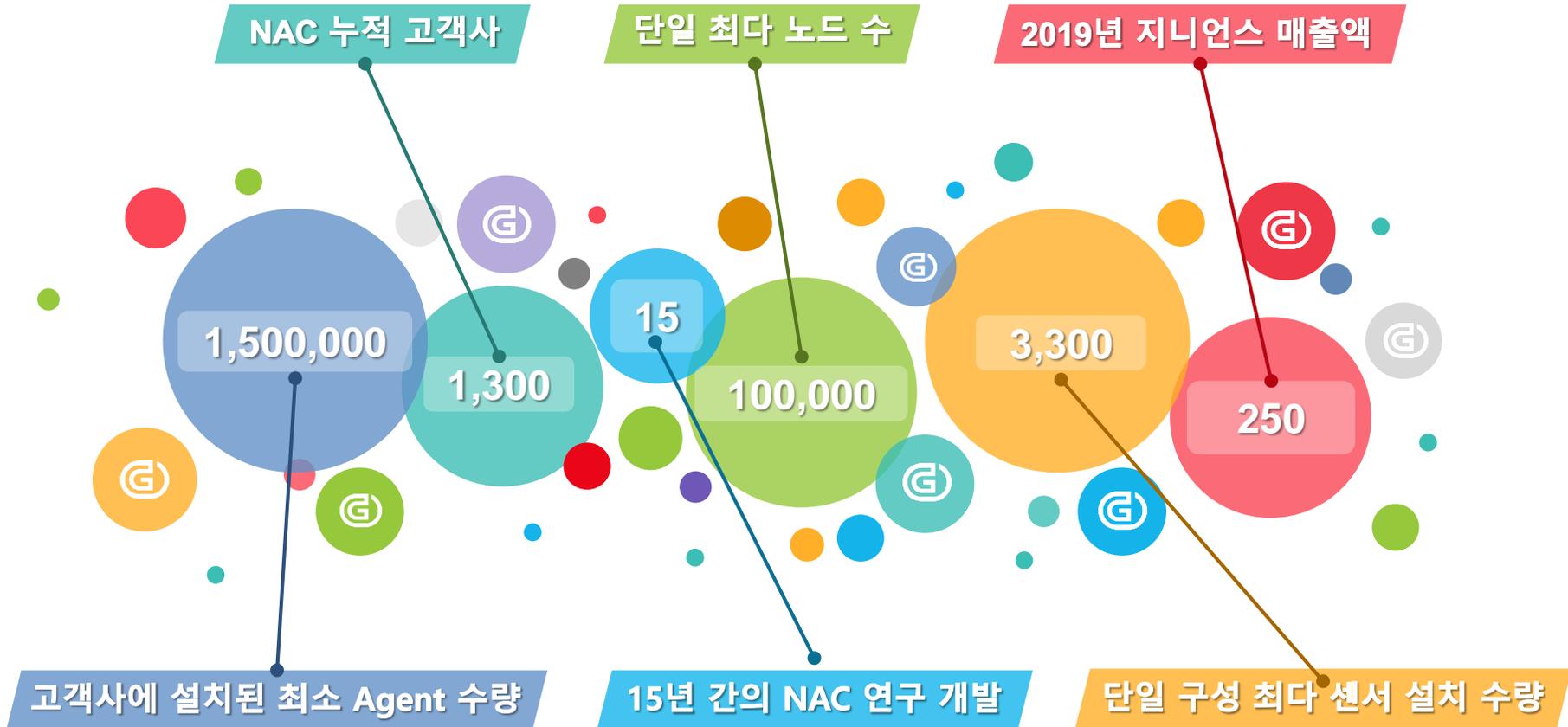
## 주 소

경기도 안양시 동안구 별말로 66  
하이필드 지식산업 A동 12층

## 홈 페이지

<http://www.genians.com>

- (주)지니언스 FACT



- 주요 고객사 현황

### 기업

HYUNDAI KIA MOTORS, LG화학, 현대중공업, SK 아이닉스, LG하우시스, DSME 대우조선해양, KCC, 동아제약, ILDONG 일등제약, SAMSUNG 에스원, SAMSUNG DISPLAY, SAMSUNG 제일모직, LOTTE Homeshopping, 롯데아사히주류, 하이마트, 중앙일보, KBS, S-OIL, ORION, woongjin 농진직용, Domino's, 동양시멘트, E-LAND, BGF리테일 CU, OLYMPUS, 삼성서울병원, 서울아산병원, 고려대학교의료원

### 금융

KEB하나은행, 우리은행, IBK기업은행, Standard Chartered, MG새마을금고, 신한, 좋은일이 생깁니다 경남은행, 광주은행, 신한저축은행, 신인지축은행, BS저축은행, 흥국생명, 현대해상, 한화손해보험, 동부화재, 신한생명 SHINHAN LIFE, 동양생명, ING, 메리츠화재, KB생명, The K 손해보험(주), 금융결제원, 우리카드, 하나카드, Mirae Asset 미래에셋생명, Hyundai Card, 비씨카드, 현대증권, NH투자증권, KDB대우증권, 아주캐피탈

### 공공기관

ncis 정부통합전산센터, 우편사업본부 KOREA POST, 한국도로공사, K water, 한국철도시설공단, KoROAD 도로교통공단, BPA 부산항만공사, 건강보험심사평가원, KBS, 법무부, 중소기업청 Small & Medium Business Administration, RDA 농촌진흥청, 경찰청, 한국은행, NOC 한국석유공사, 한국소비자원 Korea Consumer Agency, 농림축산식품부, 근로복지공단, 조달청, 내리실업 지원장소, 국회사무처, 한국전력공사, 국민건강보험, 조달청, h-well 국민건강보험, 전력거래소 KPX, 5678 문화나눔재단, 서울도시발전도, 한국에너지공단, 관세청 KOREA CUSTOMS SERVICE, 국토교통부, 국립수산물안전관리원, 환경부, KOMSCO 한국조폐공사



Thank you!