Cloud

Genian NAC

Genian NAC

01 개요

03 Cloud NAC ?

03 Cloud NAC 제품 소개

04 회사 소개

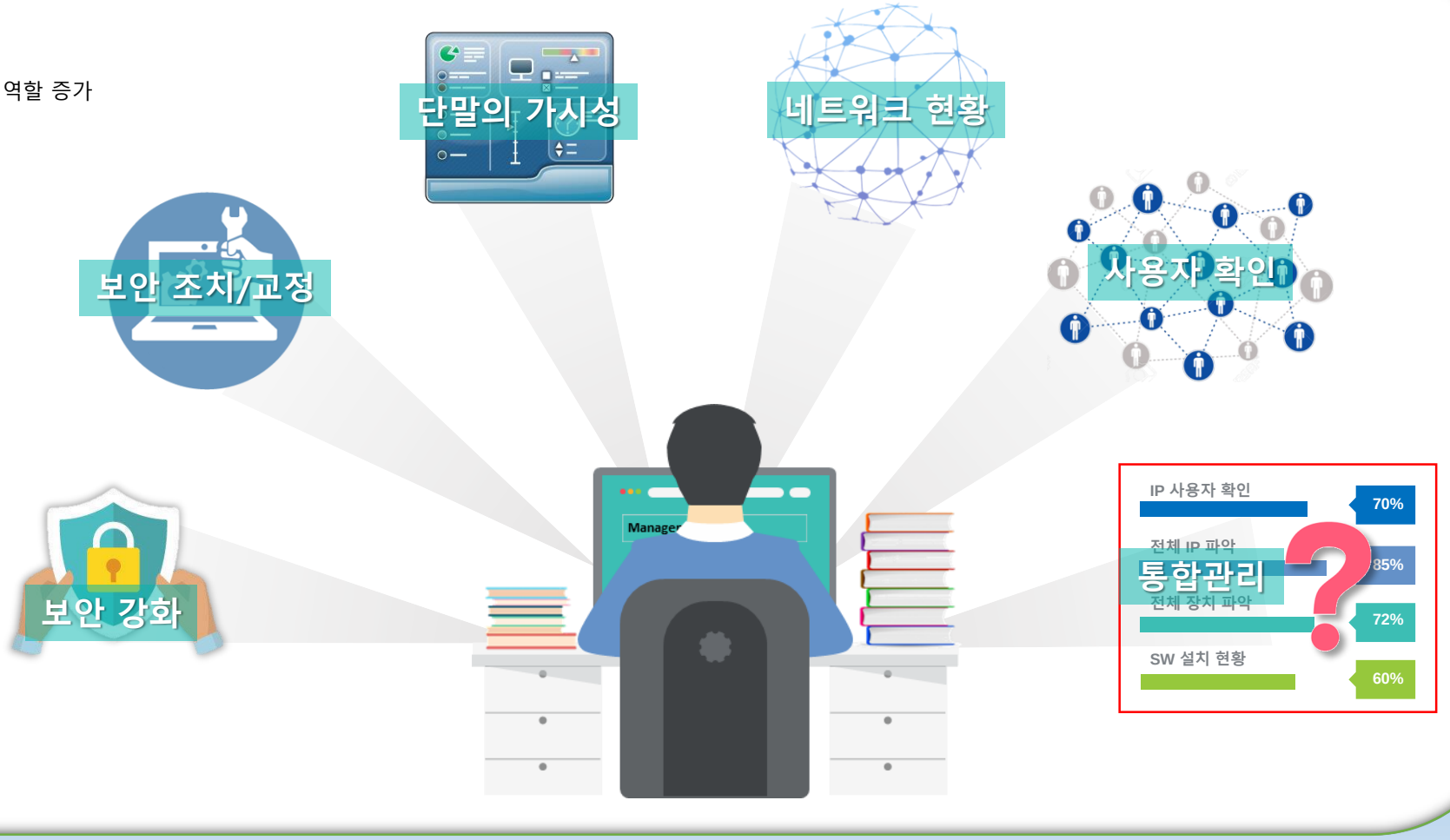
Genian NAC

개요

01 개요

- **관리 부서의 고민**

- 지속적인 보안사고로 인한 관리부서(자)의 역할 증가

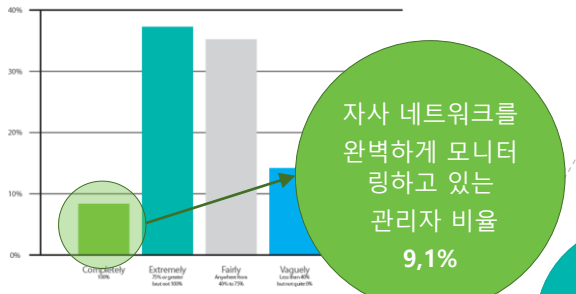


01 개요

- **내부보안? 가시성(Visibility) 확보!**

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

네트워크 가시성



자사 네트워크를 완벽하게 모니터링하고 있는 관리자 비율 **9,1%**

<출처 : SANS BYOD Security Survey>

네트워크 단말의 수량 및 다양성 증가

단말 가시성

악성코드에 감염된 단말은 아닐까?

테더링을 사용하고 있는지 않을까?

단말의 운영체제는 무엇인지!

사내 규정에 맞춘 소프트웨어를 사용하고 있는가!

무선? 유선? 무엇을 사용하고 있는지

단말의 보안 패치는 최신인지!

사용자 가시성

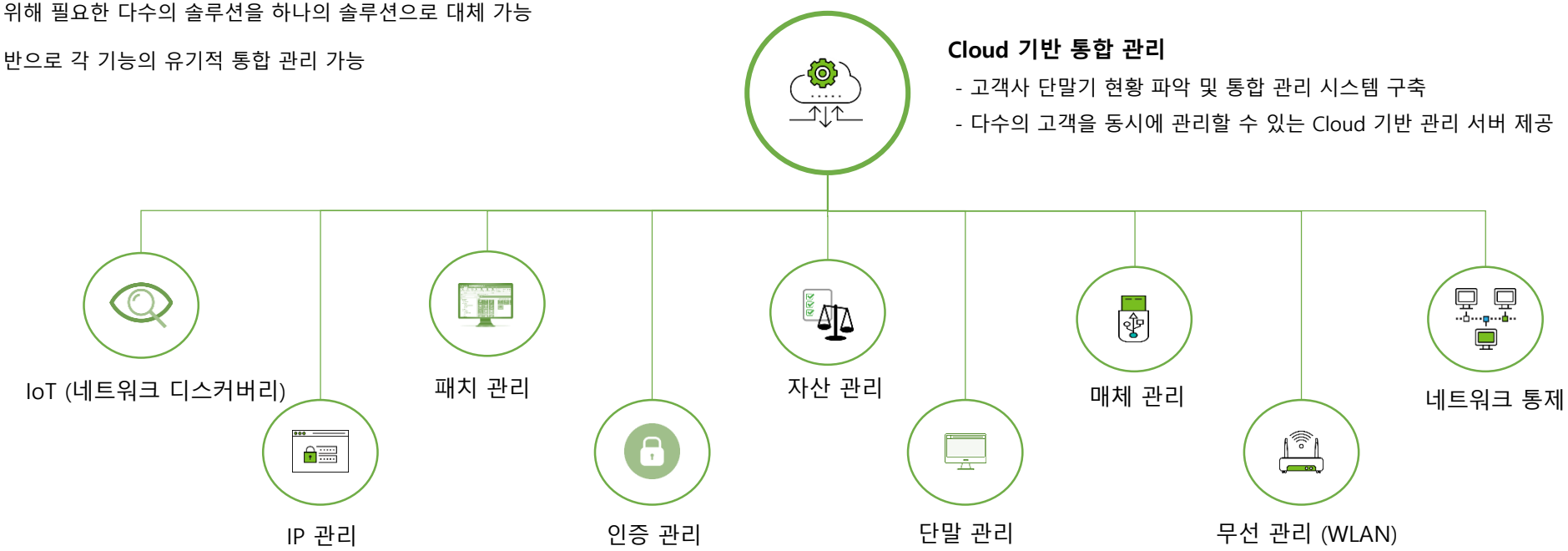
Genian NAC

Cloud NAC ?

03 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



02 Cloud NAC ?

- **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

02 Cloud NAC ?

- **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

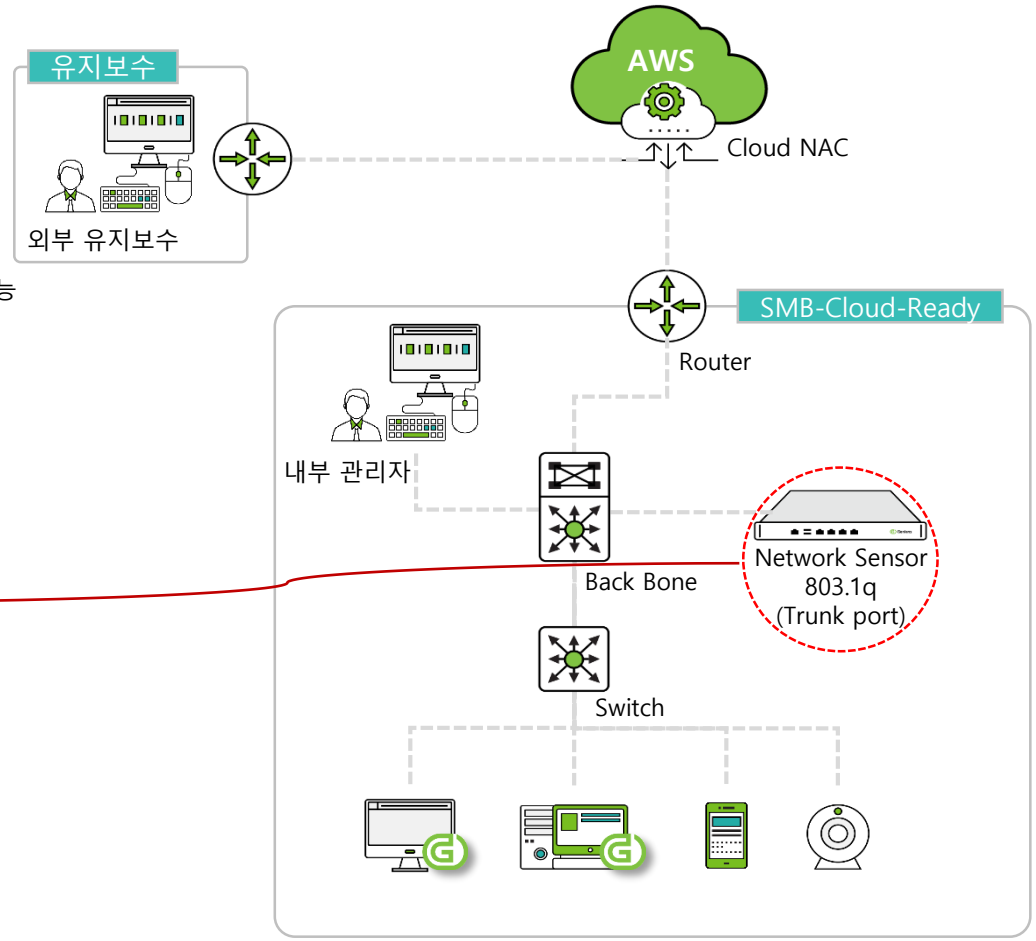
구분	지원 플랫폼	세부 지원 사양
① 정책서버 (Policy Server)	CLOUD	AWS, AZURE(US, Korea, Singapore Region)
	COTS(Commercial Off-The-Shelf)	Intel Server (HP, DELL)
	가상머신(VM)	VMWARE, KVM
	컨테이너	DOCKER
	White Labeled	사업자 전용 H/W
② 차단센서 (NetworkSensor)	전용 Appliance	X86기반 임베디드(Custom OS + Network Sensor)
	COTS	MiniPC, (Intel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

02 Cloud NAC ?

- **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

02 Cloud NAC ?

- **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

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

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

PMS (패치 관리)

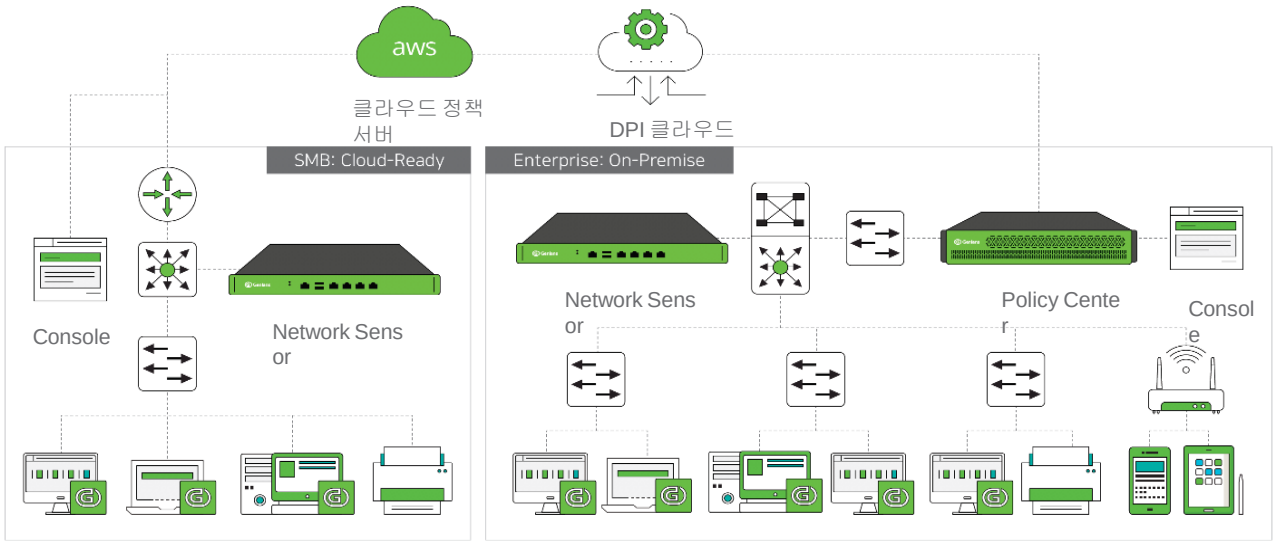
- WSUS 기반 MS Windows 및 Office 패치 관리
- 일반 파일 배포 및 설치 지원
- 망 분리(폐쇄망) 환경 지원

WLAN (무선 관리)

- SSID 및 SSID 별 접속 단말 현황 파악
- 불법(rogue) AP 및 SoftAP(핫스폿) 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



Genian NAC

Cloud NAC 제품소개

03 Cloud NAC 제품 소개

- **관리 툴을 넘어선 필수 인프라 NAC**

- 접근 제어의 필수 요소인 다양한 가시성을 통한 분류와 통제

03 Cloud NAC 제품 소개

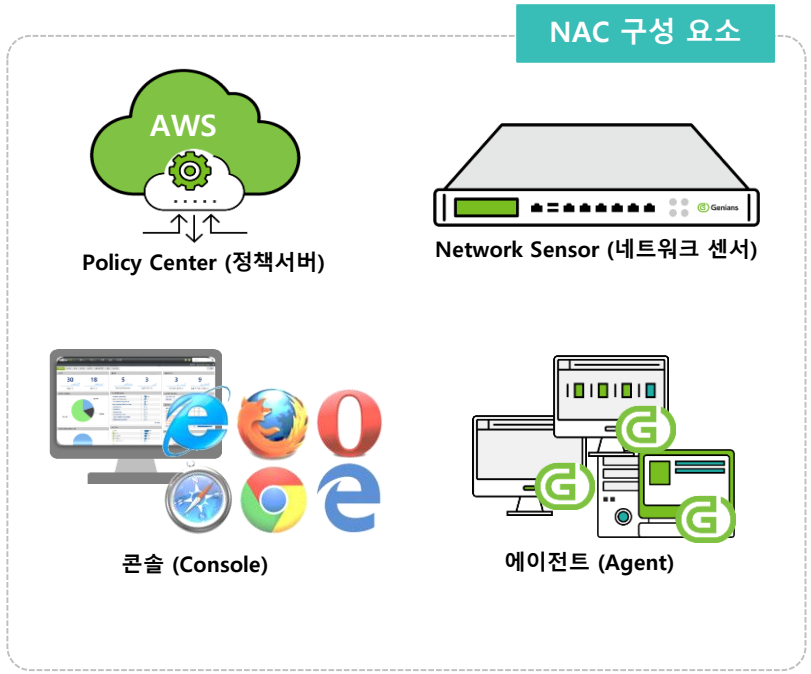
- **Cloud NAC 구성 (1/3)**

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

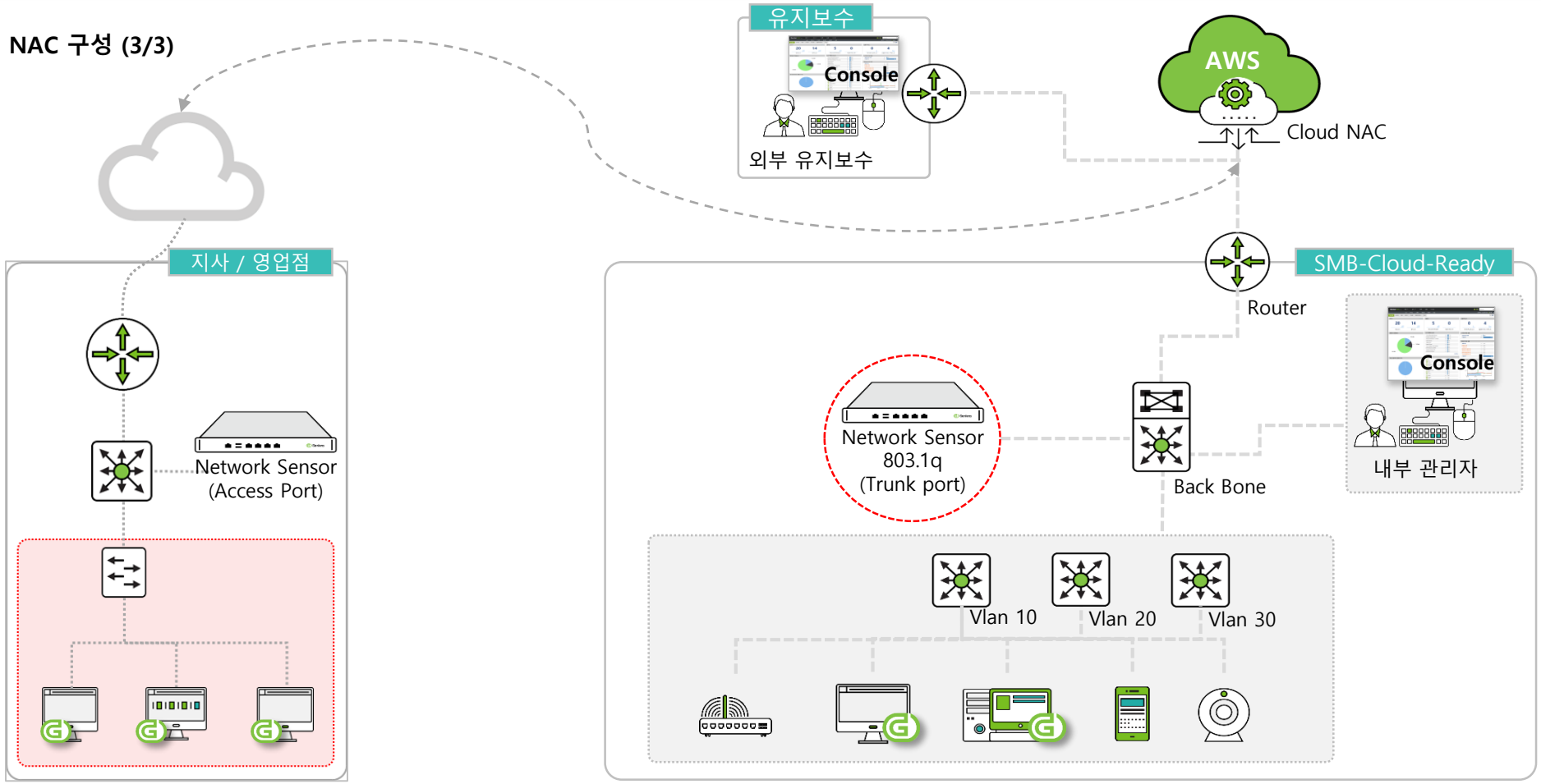
- **Cloud NAC 구성 (2/3)**

항목	종류						설명
Policy Center (정책 서버)	100 Node	200 Node	300 Node			-	- 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

03 Cloud NAC 제품 소개

- **Cloud NAC 구성 (3/3)**



03 Cloud NAC 제품 소개

- **가시성 (1/3)**

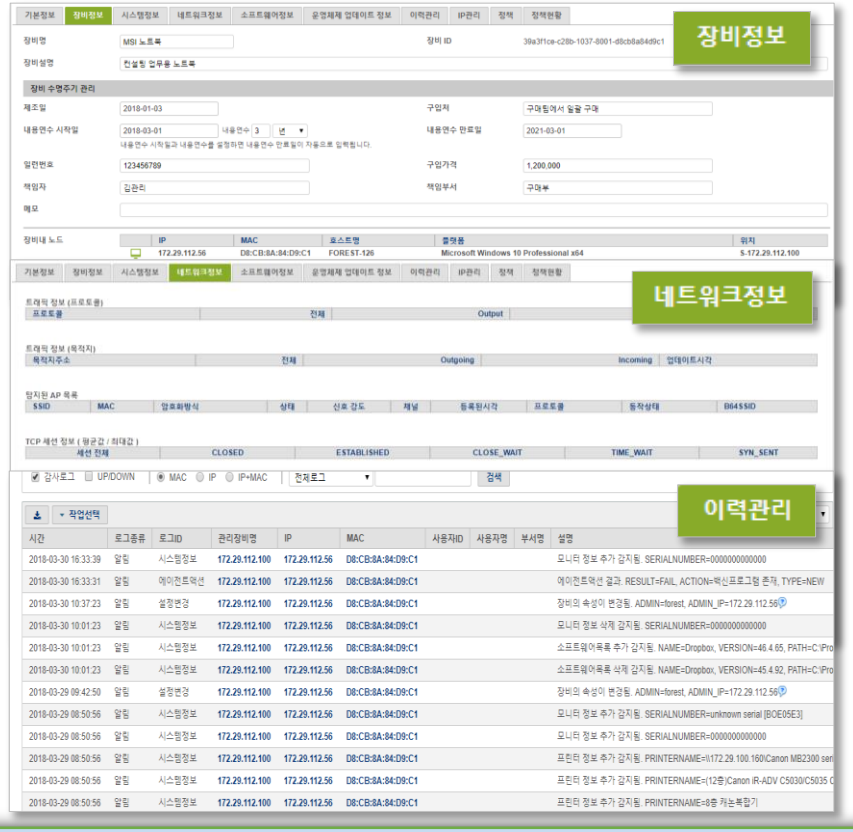
- 네트워크 내의 모든 단말기 정보 수집 및 분류, IP 실명 확인

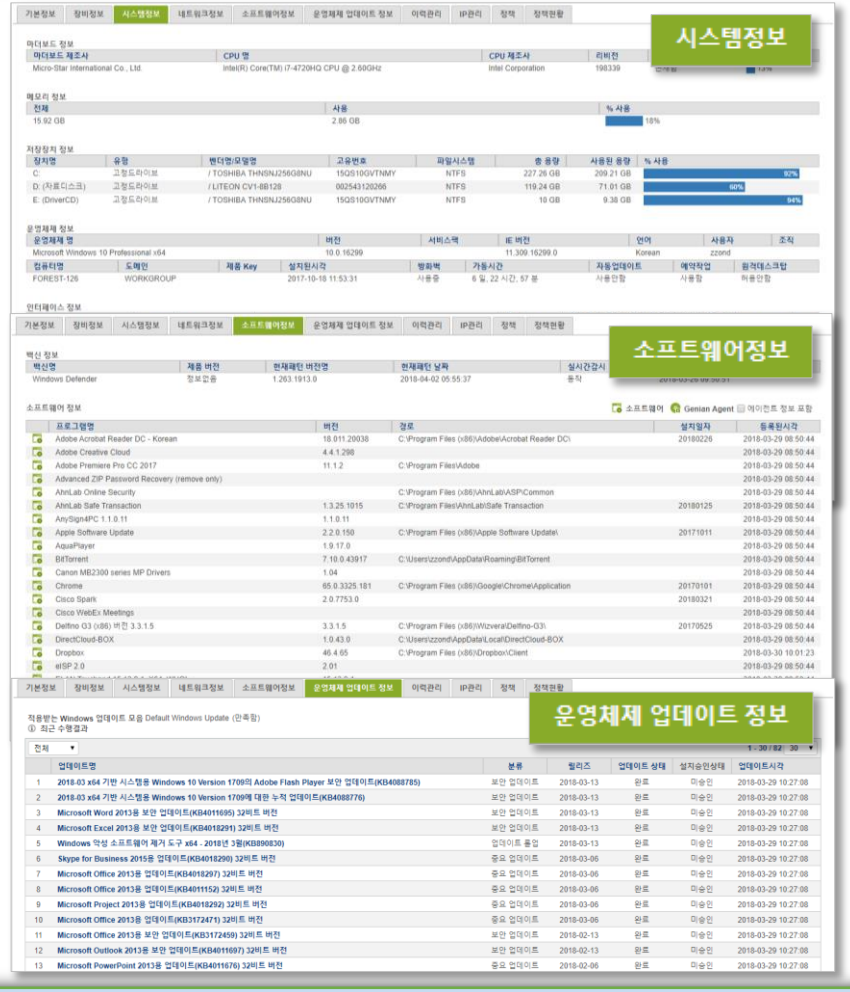
장치 구분	On/Off	가동률	인증 정보	인증 시간	연결된 스위치		IP/MAC		사용 위치	OS/장치 모델 상세 정보	서비스	최종연결시간	Hostname	NIC 제조사	동작 현황
NT AG SS	동작	가동률	인증사용자	최근 사용자인증	스위치	포트	IP주소	MAC주소	위치	플랫폼	서비스	마지막 동작시각	호스트명	NIC벤더	동작상태차트
		22%	황	2018-04-05 15:29:09			172.29.50.158	E4:70:B8:EE:5B:33	50.0 연구소IP대역	Microsoft Windows 10 Home x64			DESKTOP-9KISQBM	Intel Corporate	
		16%	황	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			DESKTOP-9KISQBM	REALTEK SEMICONDUCTOR CORP.	
		19%	현	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			android-4d2a63951ba29b9d	LG Electronics (Mobile Communications)	
		32%	허	2018-04-04 17:05:28	172.29.50.6	1	172.29.50.229	E8:3A:12:1C:08:DB	50.0 연구소IP대역	Samsung GALAXY S6 Phone		2018-04-04 17:32:52	Android	Samsung Electronics Co.,Ltd	
		2%	허	2018-04-03 12:36:59			172.29.50.219	80:E6:50:0F:5D:B8	50.0 연구소IP대역	Apple MacBook Pro		2018-04-03 09:55:19	MACBOOKPRO-5DB8	Apple, Inc.	
		20%	허	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		2018-04-04 17:28:52	KEVIN	Hon Hai Precision Ind. Co.,Ltd.	
		29%	한	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		2018-04-05 15:03:30	HKHAN	REALTEK SEMICONDUCTOR CORP.	
		20%	하	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			DESKTOP-CR1H8TU	ASRock Incorporation	
		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			Playdesignin	Apple, Inc.	
		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			JUNSUK-NOTEBOOK	REALTEK SEMICONDUCTOR CORP.	
		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		2018-04-02 21:53:13	YOUSINNOTE	Intel Corporate	
		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			DESKTOP-UMVOTUM	GIGA-BYTE TECHNOLOGY CO.,LTD.	
		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		2018-04-05 15:26:34	iPhone8	Apple, Inc.	
		0%	진	2018-04-03 10:24:19			172.29.100.138	AC:BC:32:D6:1D:43	100.4(12층 서버실)	Apple MacBook Pro		2018-03-29 17:41:55	MACBOOKPRO-1D43	Apple, Inc.	
		100%	진	2018-04-03 10:24:19			172.29.50.234	AC:BC:32:D6:1D:43	50.0 연구소IP대역	Apple MacBook Pro			MACBOOKPRO-1D43	Apple, Inc.	
		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			YSJIN-WIN10	Micro-Star INT'L CO., LTD	
		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		2018-04-05 11:34:33	jomyeongjin	Apple, Inc.	
		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			DESKTOP-ET619IN	GIGA-BYTE TECHNOLOGY CO.,LTD.	
		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			DESKTOP-E125H95	GIGA-BYTE TECHNOLOGY CO.,LTD.	
		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			COM-PC	GIGA-BYTE TECHNOLOGY CO.,LTD.	
		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			A-PC	GIGA-BYTE TECHNOLOGY CO.,LTD.	
		100%	장	2018-04-03 10:33:47			172.29.50.176	B8:E8:56:04:B6:B0	50.0 연구소IP대역	Apple MacBook Air		2018-04-05 14:24:04	MACBOOKAIR-B6B0	Apple, Inc.	
		11%	장	2018-04-03 10:33:47			172.29.60.55	B8:E8:56:04:B6:B0	60.0 (AGENT팀)	Apple MacBook Air		2018-04-05 10:22:48	MACBOOKAIR-B6B0	Apple, Inc.	
		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			DESKTOP-31UAUFT	VMware, Inc.	
		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			android-898795b18a1e896	LG Electronics (Mobile Communications)	
		85%	임	2018-02-19 07:54:35			172.29.50.239	40:8D:5C:79:FD:85	50.0 연구소IP대역	Microsoft Windows 10 Home x64			WISEMANLIM-GENI	GIGA-BYTE TECHNOLOGY CO.,LTD.	
		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		2018-04-05 10:57:21	DESKTOP-YIHO25	Intel Corporate	
		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		2018-04-05 10:56:51	DESKTOP-YIHO25	Dell Inc.	

03 Cloud NAC 제품 소개

- **가시성 (2/3)**

- 단말 내 다양한 정보 제공

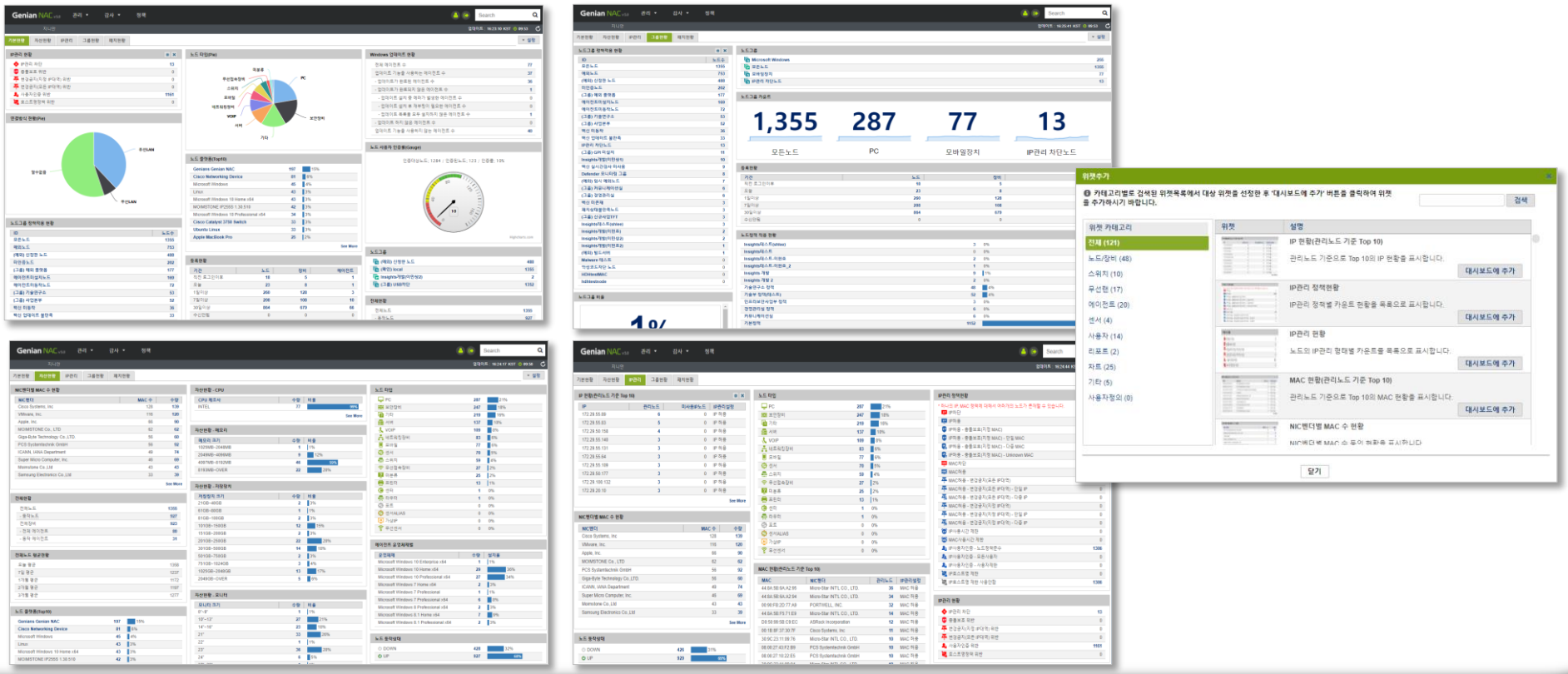




03 Cloud NAC 제품 소개

- **가시성 (3/3)**

- Dashboard를 통한 다양한 통계, 상태 등의 현황 파악에 용이



03 Cloud NAC 제품 소개

- **분류 (1/2)**

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

그룹 조건 예시

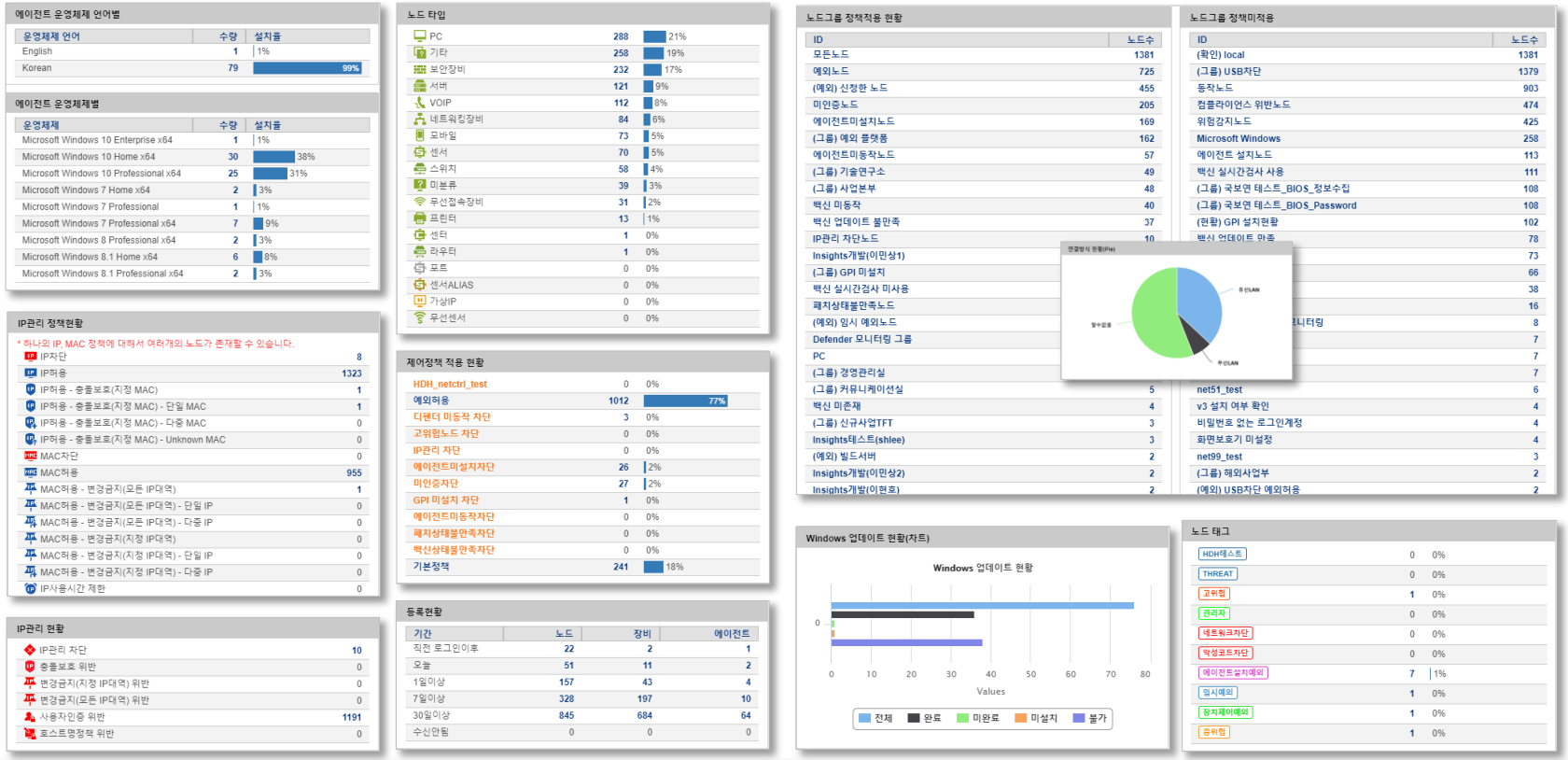
IP관리 / 상태 / **차단됨**
플랫폼 / 감지된 플랫폼에 문자열 포함하면 / **Microsoft Windows**
장비내 무선랜 / 무선랜그룹에 속하는 AP가 존재하면 /
접속AP / 무선랜그룹에 속하면 /
USB 장치 정보 / 장치명이 문자열을 포함하면 / **WebCam**
구입가격 / 보다 비싸면 / **1000000**
업/다운상태 / 상태값 / **UP**
노드타입 / 감지된 노드타입이 같으면 / **모바일**
인증사용자 / 인증상태 / **인증되지 않음**
백신정보 / 최근검사 시각이 보다 이내이면 / **1 주, 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**
노드그룹 / 속하면 / **Microsoft Windows** 에이전트상태 / 설치상태 / **설치안됨**
위험감지 / 노드에 감지된 위험이 / **감지되면**
시스템 / Windows 방화벽 / **사용안함**

분류 조건

03 Cloud NAC 제품 소개

- **분류 (2/2)**

- Dashboard를 통한 다양한 통계, 상태 등의 현황 파악에 용이



에이전트 운영체제 언어별

운영체제 언어	수량	설치율
English	1	1%
Korean	79	99%

에이전트 운영체제별

운영체제	수량	설치율
Microsoft Windows 10 Enterprise x64	1	1%
Microsoft Windows 10 Home x64	30	38%
Microsoft Windows 10 Professional x64	25	31%
Microsoft Windows 7 Home x64	2	3%
Microsoft Windows 7 Professional	1	1%
Microsoft Windows 7 Professional x64	7	9%
Microsoft Windows 8 Professional x64	2	3%
Microsoft Windows 8.1 Home x64	6	8%
Microsoft Windows 8.1 Professional x64	2	3%

IP관리 정책현황

* 하나의 IP, MAC 정책에 대해서 여러개의 노드가 존재할 수 있습니다.

IP차단	8
IP허용	1323
IP허용 - 충돌보호(지정 MAC)	1
IP허용 - 충돌보호(지정 MAC) - 단일 MAC	1
IP허용 - 충돌보호(지정 MAC) - 다중 MAC	0
IP허용 - 충돌보호(지정 MAC) - Unknown MAC	0
MAC차단	0
MAC허용	955
MAC허용 - 변경금지(모든 IP대역)	1
MAC허용 - 변경금지(모든 IP대역) - 단일 IP	0
MAC허용 - 변경금지(모든 IP대역) - 다중 IP	0
MAC허용 - 변경금지(지정 IP대역)	0
MAC허용 - 변경금지(지정 IP대역) - 단일 IP	0
MAC허용 - 변경금지(지정 IP대역) - 다중 IP	0
IP사용시간 제한	0

IP관리 현황

IP관리 차단	10
충돌보호 위반	0
변경금지(지정 IP대역) 위반	0
변경금지(모든 IP대역) 위반	0
사용자인증 위반	1191
호스트명정책 위반	0

노드 타입

PC	288	21%
기타	258	19%
보안장비	232	17%
서버	121	9%
VOIP	112	8%
네트워킹장비	84	6%
모바일	73	5%
센서	70	5%
스위치	58	4%
미분류	39	3%
무선접속장비	31	2%
프린터	13	1%
센터	1	0%
라우터	1	0%
포트	0	0%
센서ALIAS	0	0%
가상IP	0	0%
무선센서	0	0%

제어정책 적용 현황

HDH_netctrl_test	0	0%
예외허용	1012	77%
디렌더 미동작 차단	3	0%
고위험노드 차단	0	0%
IP관리 차단	0	0%
에이전트미설치차단	26	2%
미인증차단	27	2%
GPI 미설치 차단	1	0%
에이전트미동작차단	0	0%
패치상태불만족차단	0	0%
백신상태불만족차단	0	0%
기본정책	241	18%

등록현황

기간	노드	장비	에이전트
직전 로그인이후	22	2	1
오늘	51	11	2
1일이상	157	43	4
7일이상	328	197	10
30일이상	845	684	64
수신안됨	0	0	0

노드그룹 정책적용 현황

ID	노드수
모든노드	1381
예외노드	725
(예외) 신청한 노드	455
미인증노드	205
에이전트미설치노드	169
(그룹) 예외 플랫폼	162
에이전트미동작노드	57
(그룹) 기술연구소	49
(그룹) 사업본부	48
백신 미동작	40
백신 업데이트 불만족	37
IP관리 차단노드	10
Insights개발(이민상1)	
(그룹) GPI 미설치	
백신 실시간검사 미사용	
패치상태불만족노드	
(예외) 임시 예외노드	
Defender 모니터링 그룹	
PC	
(그룹) 경영관리실	
(그룹) 커뮤니케이션실	5
백신 미존재	4
(그룹) 신규사업TFT	3
Insights테스트(shlee)	3
(예외) 빌드서버	2
Insights개발(이민상2)	2
Insights개발(이현호)	2

노드그룹 정책미적용

ID	노드수
(확인) local	1381
(그룹) USB차단	1379
동작노드	903
컴플라이언스 위반노드	474
위험감지노드	425
Microsoft Windows	258
에이전트 설치노드	113
백신 실시간검사 사용	111
(그룹) 국보연 테스트_BIOS_정보수집	108
(그룹) 국보연 테스트_BIOS_Password	108
(현황) GPI 설치현황	102
백신 업데이트 만족	78
	73
	66
	38
	16
모니터링	8
	7
	7
	7
net51_test	6
v3 설치 여부 확인	4
비밀번호 없는 로그인계정	4
화면보호기 미설정	4
net99_test	3
(그룹) 해외사업부	2
(예외) USB차단 예외허용	2

Windows 업데이트 현황(차트)

노드 태그

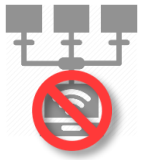
HDH테스트	0	0%
THREAT	0	0%
고위험	1	0%
관리자	0	0%
네트워크차단	0	0%
악성코드차단	0	0%
에이전트설치예외	7	1%
임시예외	1	0%
장치제어예외	1	0%
중위험	1	0%

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)

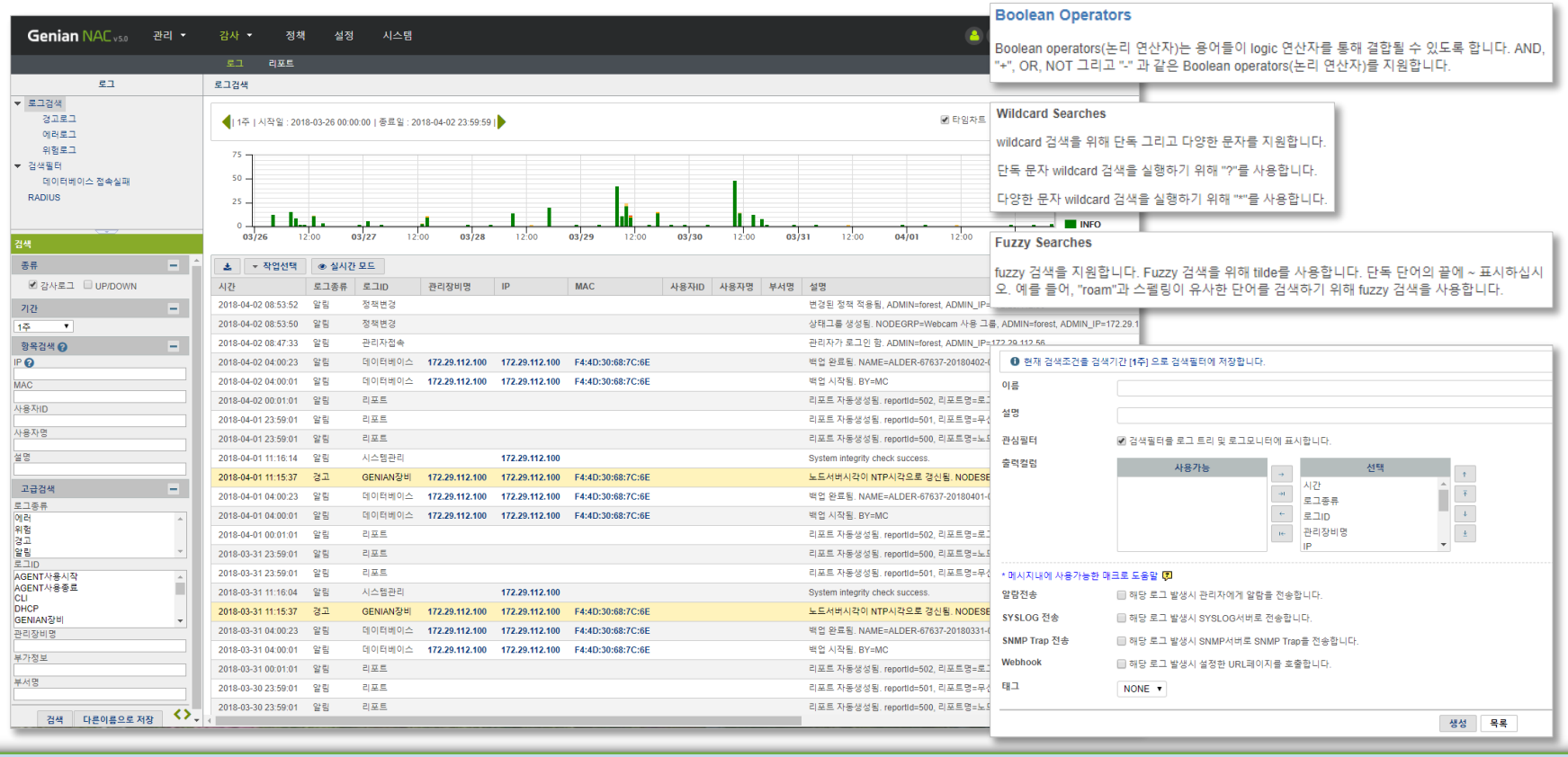
불법 SW 삭제
(허용되지 않은 특정
SW 강제 삭제)

보안 설정 강제화
(패스워드 설정 유도,
화면보호기 강제 설정 등)

03 Cloud NAC 제품 소개

- **리포트 (1/2)**

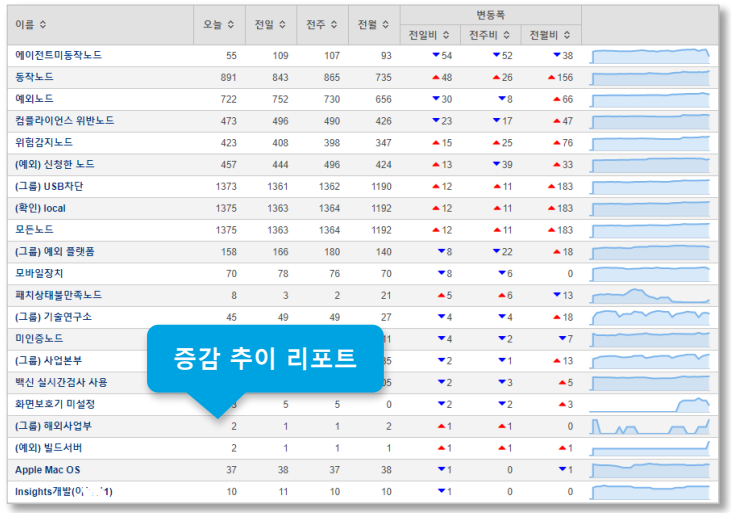
- 감사로그 필터링 & 로그 전송(SMS, E-mail, Syslog, Snmptrap)

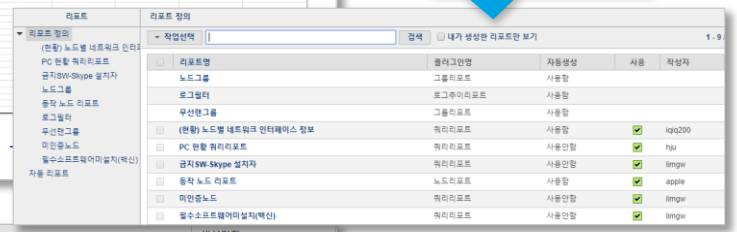


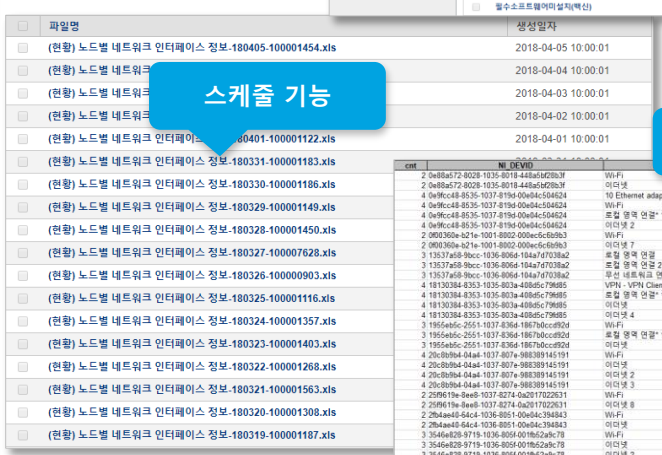
03 Cloud NAC 제품 소개

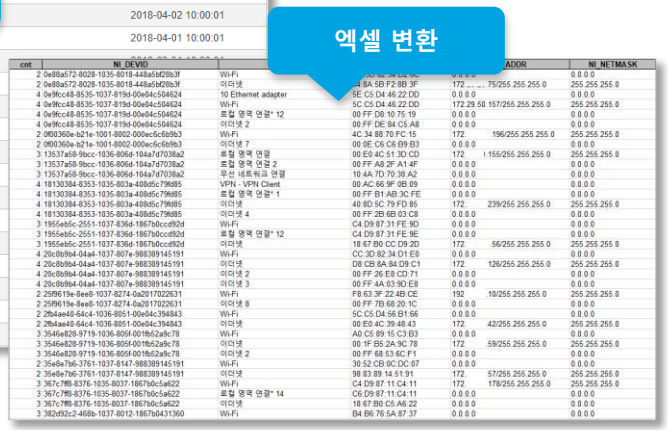
- **리포트 (2/2)**

- 노드, 쿼리, 로그 리포트 제공









03 Cloud NAC 제품 소개

- **Cloud NAC 기능 요약**

- 다양한 방식의 접근 제어 가능

Agent-less

Platform 분류	OS(Win, Linux, Unix, iOS, Android 등)별, 네트워크 장비, 프린터, 제조사 등
접근제어	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)
네트워크 정보	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

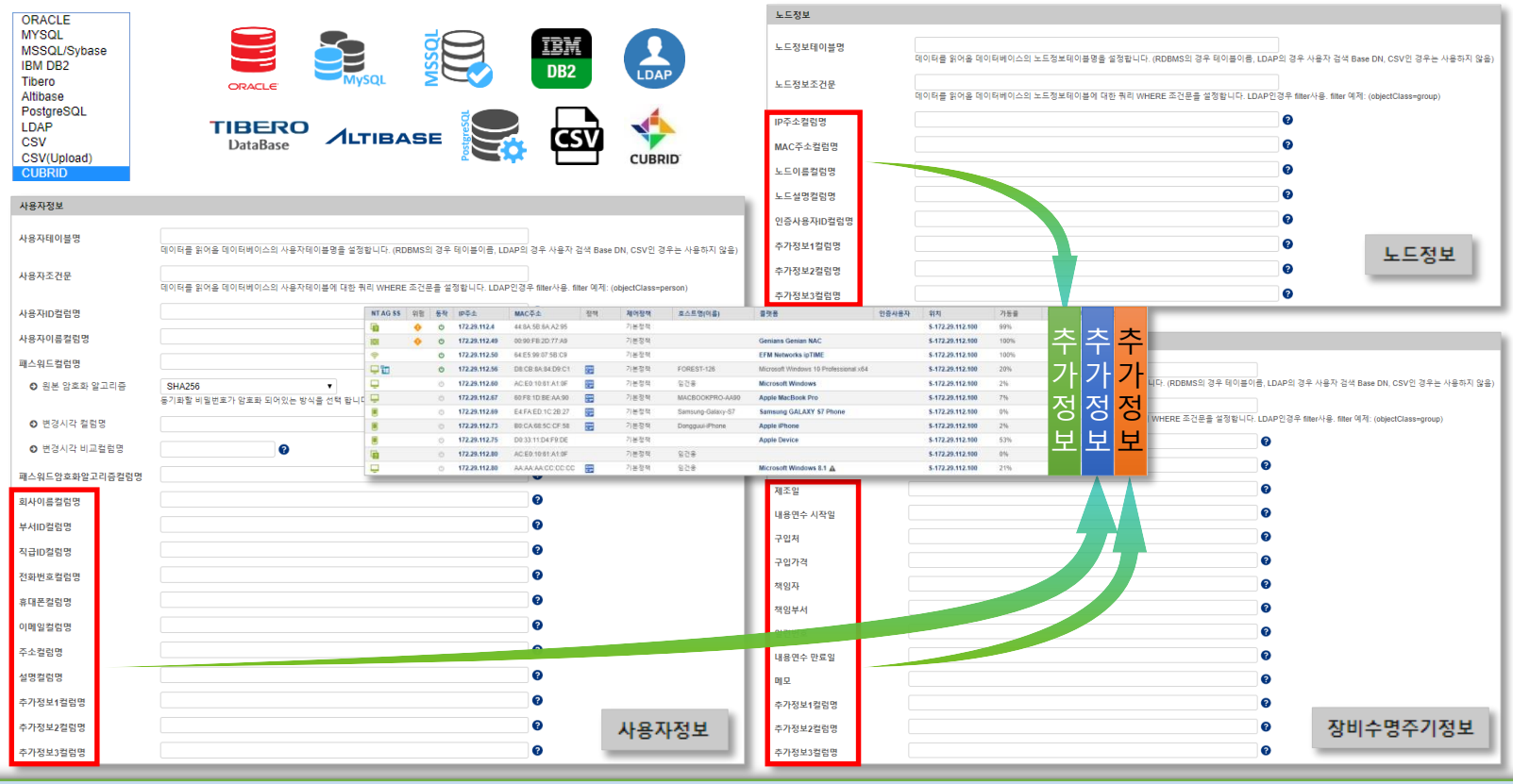
Agent

MSOS, Office 패치	Windows patch, MS office patch
시스템 정보	PC H/W 정보(CPU, MEM, DISK, OS, NIC 등), Hostname 수집 및 제어
세션 제어	TCP 세션 정보 수집 및 임계치 초과시 차단
포트 정보	열린 포트, 포트 사용 프로세스, 서비스 정보
장치제어	USB, NIC, Bluetooth, Wifi, Tethering, PC전원 제어
프로세스 제어	특정 프로세스 강제 중지
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)
보안기능	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
위 변조 탐지	IP, MAC clone 탐지/차단
AP탐지	무선 AP 탐지 및 접속 제어
시스템 정보	OS, H/W 정보(CPU, MEM, DISK, OS, NIC 등)
소프트웨어 탐지	설치된 프로그램 정보확인, 백신 정보 확인
OS 패치	MAC OS 업데이트

03 Cloud NAC 제품 소개

- **Cloud NAC 제품 특장점**

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



03 Cloud NAC 제품 소개

- **Cloud NAC 제품 특장점**

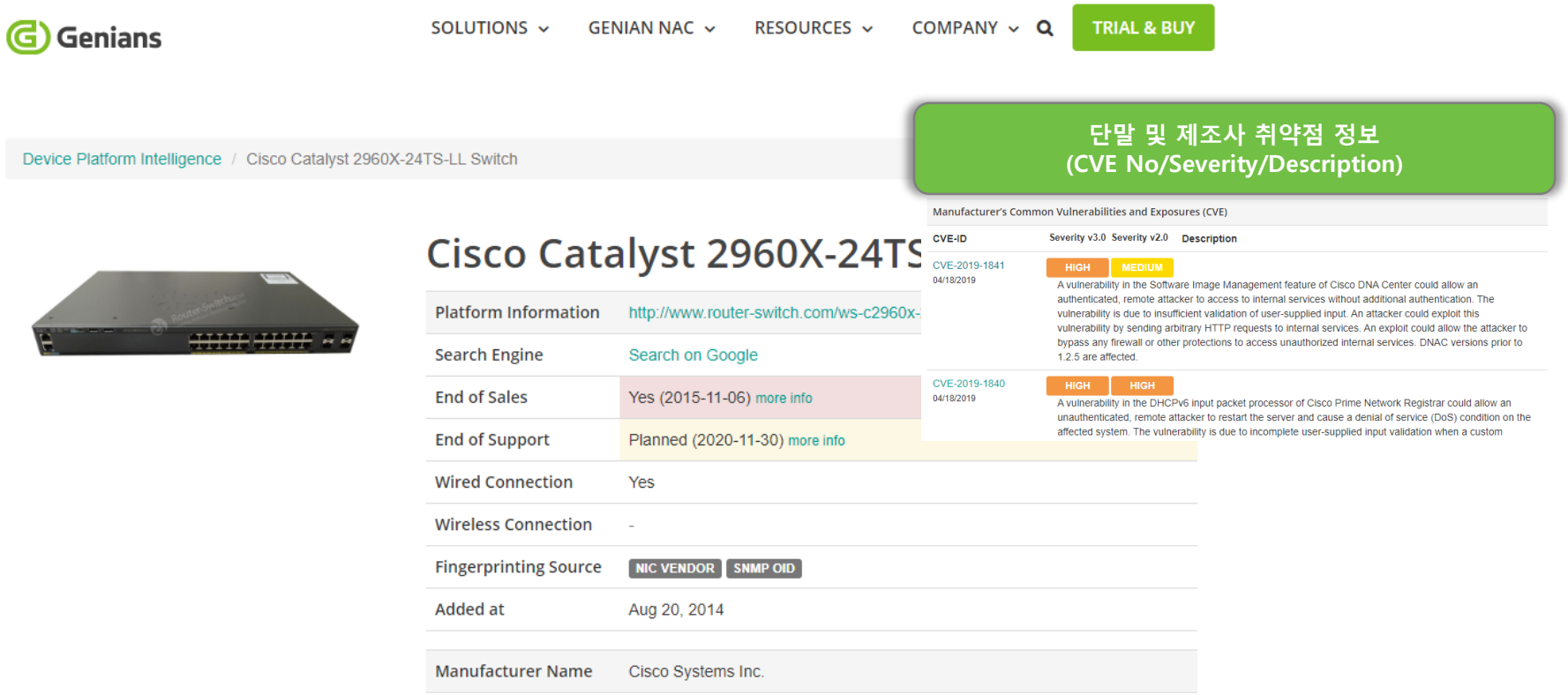
- 장비 수명주기 관리 기능 제공

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

03 Cloud NAC 제품 소개

- **Cloud NAC 제품 특장점**

- 플랫폼 자동 분류 기능 단말 플랫폼 인텔리전스 (DPI) 제공

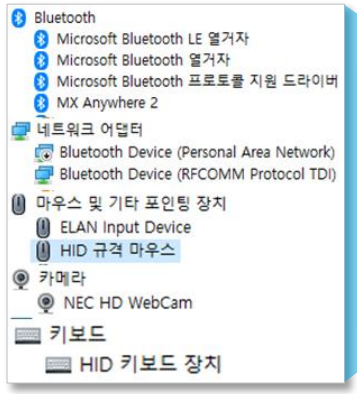


03 Cloud NAC 제품 소개

- **Cloud NAC 제품 특장점**

- USB 장치 정보 자동 수집 및 조건 설정 그룹 생성

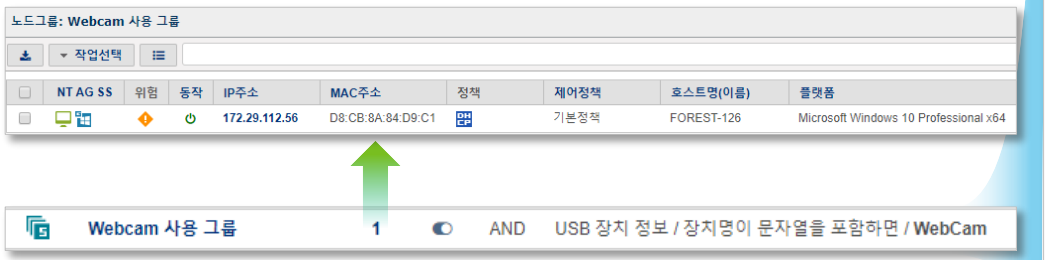
장치정보

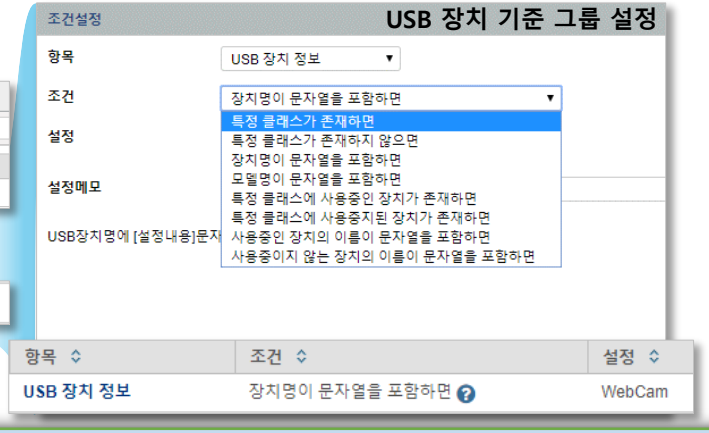


NAC 에 등록된 USB 정보

USB 정보

클래스명	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

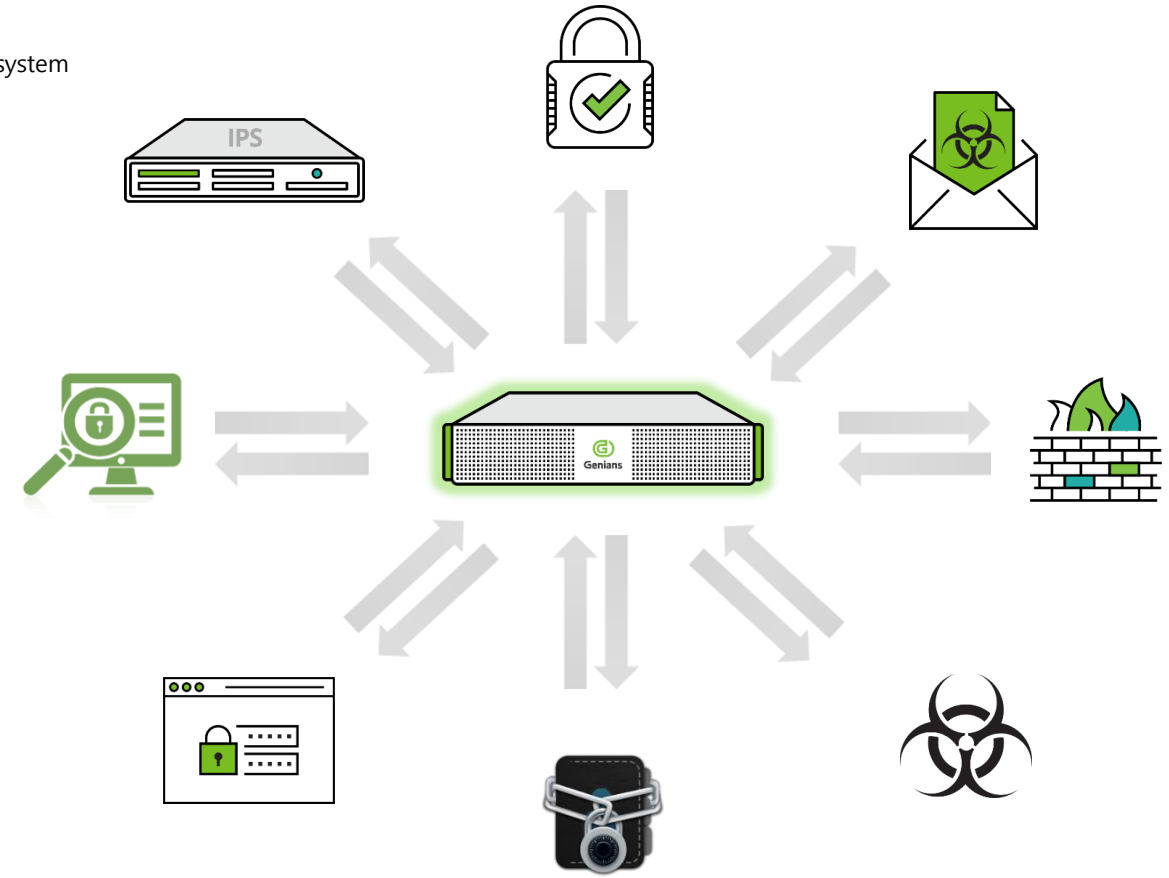




03 Cloud NAC 제품 소개

- **Cloud NAC 제품 특장점**

- 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

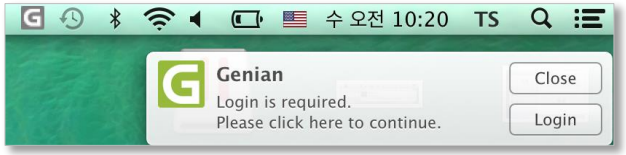
4. DB 연동
   - DB 연동으로 추가적인 정보 제공

03 Cloud NAC 제품 소개

- **Cloud NAC 제품 특장점**

- MAC OS (OSX) Agent 지원

OSX Agent 설치 화면



OSX 로그인 팝업

OSX 노드 정보

172.29.112.60	AC:E0:10:61:A1:0F		기본정책	임	Microsoft Windows
172.29.112.61	80:E6:50:0F:5F:6C		기본정책	gunwoongui-macbook-pro.local	Apple OS X Mavericks
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 노드정보에 표시합니다.
		하드웨어정보 수집	하드웨어정보 수집	마더보드 정보, 메모리정보, 저장장치 정보를 수집하여 노드정보에 표시합니다.
		소프트웨어정보 수집	소프트웨어정보 수집	설치된 소프트웨어정보를 수집하여 노드정보의 [소프트웨어정보]-[소프트웨어목록]에 표시합니다.
		네트워크정보 수집	네트워크정보 수집	네트워크 인터페이스 정보를 수집하여 노드정보에 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

OSX 지원 버전

- 전체
- Apple OS X Mavericks
- Apple OS X El Capitan
- Apple macOS High Sierra
- Apple OS X Yosemite
- Apple macOS Sierra

백신 정보

백신명	제품 버전	최근검사시간

소프트웨어 정보

프로그램명	버전			최근변경시각	등록된시각
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	/Applications/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	/System/Library/CoreServices/Feedback Assistant.app	3/23/14, 4:56 AM	2018-04-04 09:38:54

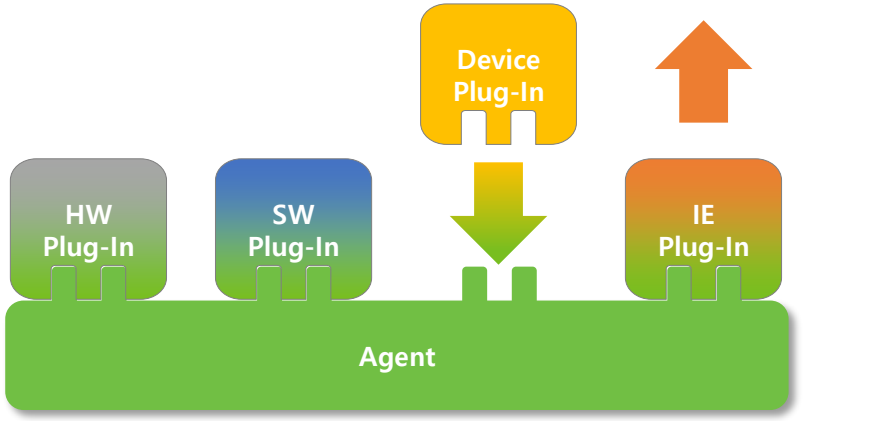
03 Cloud NAC 제품 소개

- **Cloud NAC 제품 특장점**

- 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	액션명	플러그인명	설명
		사용자 알림메시지	사용자 알림메시지	사용자에게 알림메시지를 표시합니다.
		프로그램 제거	프로그램 제거	제어판의 프로그램 제거에 등록된 프로그램중 제거 가능한 특정 프로그램을 제거합니다.
		DNS 제어	DNS 제어	DNS 관련 로컬설정을 제어합니다.
		유선랜 인증 프로파일 설정	유선랜 인증 프로파일 설정	유선인터페이스의 802.1x 인증 프로파일 설정을 강제화 한다.
		네트워크 트래픽 제어	네트워크 트래픽 제어	주기적으로 네트워크 사용량을 수집하여 설정된 수치 이상일 경우 네트워크 인터페이스를 차단합니다.
		운영체제정보 수집	운영체제정보 수집	macOS 운영체제 정보 및 사용자 정보를 수집하여 노드정보에 표시합니다.
		하드웨어정보 수집	하드웨어정보 수집	마더보드 정보, 메모리정보, 저장장치 정보를 수집하여 노드정보에 표시합니다.
		소프트웨어정보 수집	소프트웨어정보 수집	설치된 소프트웨어정보를 수집하여 노드정보의 [소프트웨어정보]-[소프트웨어목록]에 표시합니다.
		네트워크정보 수집	네트워크정보 수집	네트워크 인터페이스 정보를 수집하여 노드정보에 표시합니다.
		백신정보 수집	백신정보 수집	PC에 설치되어있는 백신프로그램 정보를 수집합니다.
		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)**

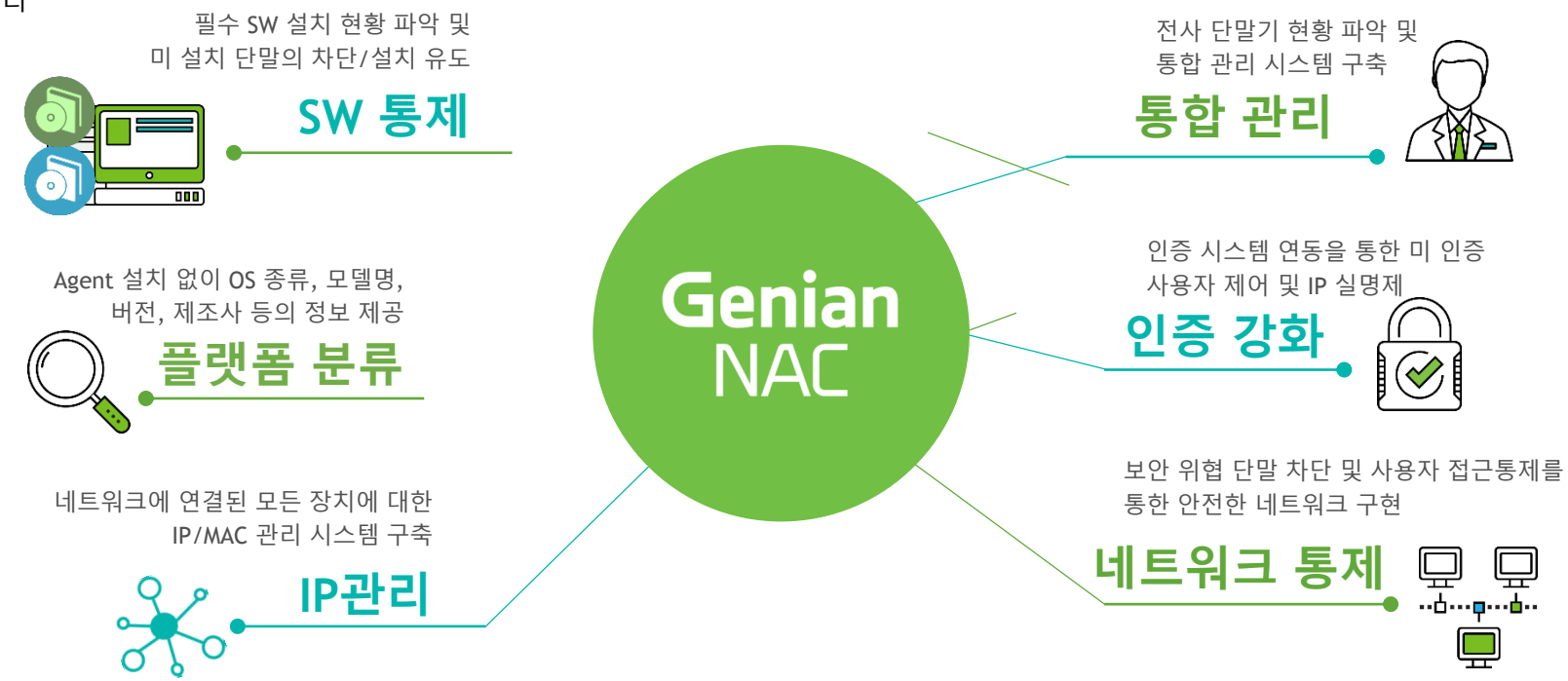
- 단계별 정책 준수 후 네트워크 허용 프로세스

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

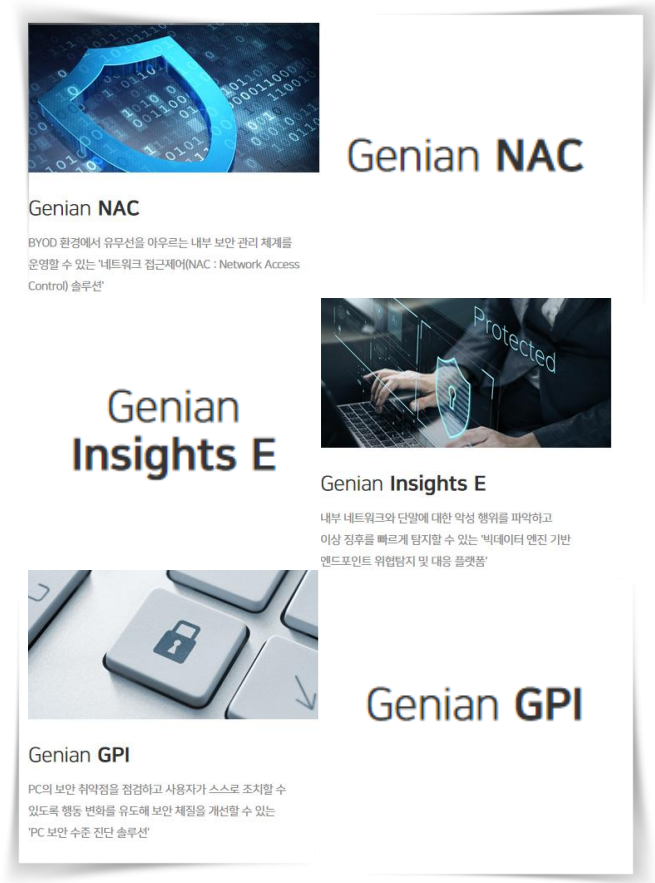


Genian NAC

회사 소개

04 회사 소개

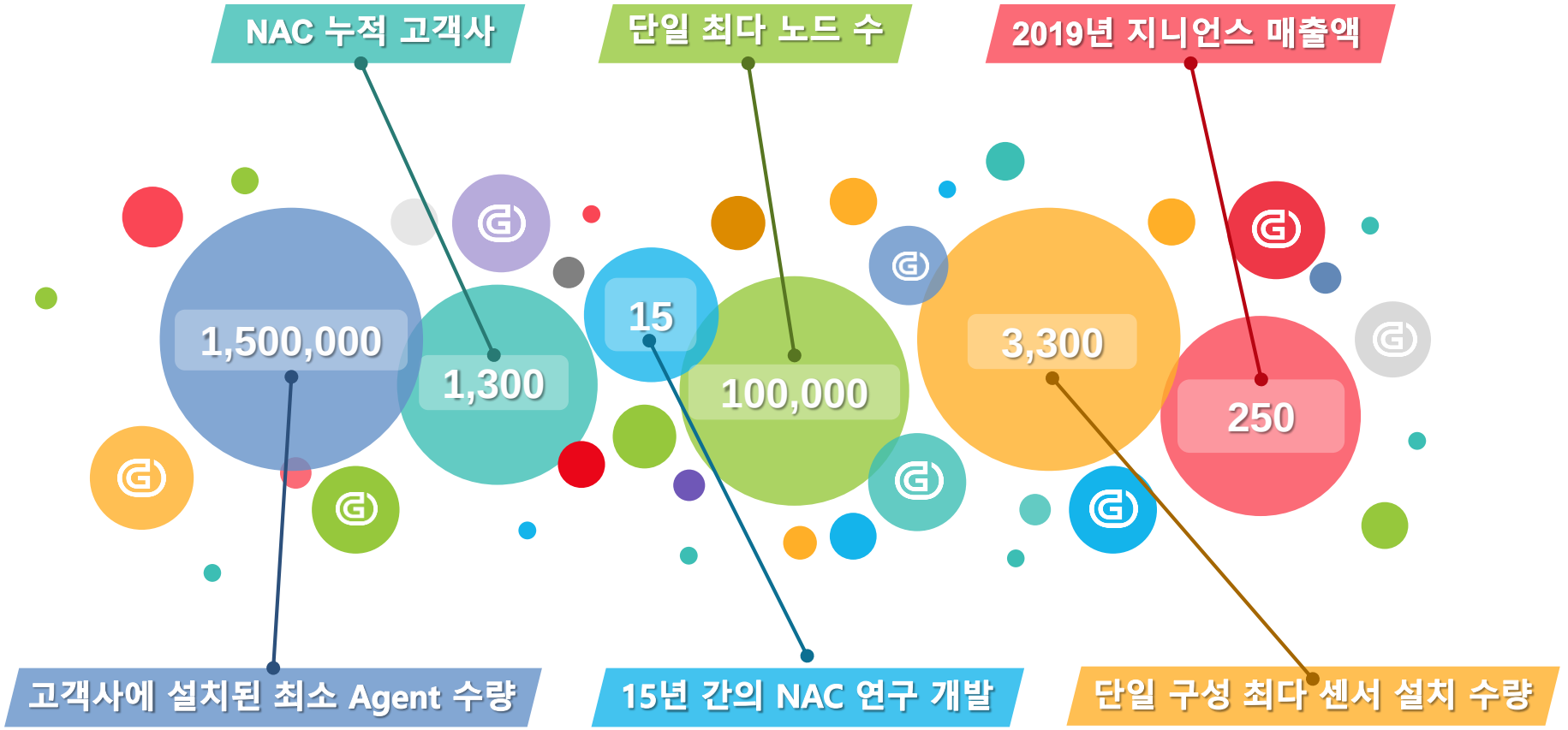
- **NAC 기술 기반 보안 플랫폼 기업 지니언스!**



회 사 명	㈜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 벌말로 66 하이필드 지식산업 A동 12층
홈 페 이 지	http://www.genians.com

04 회사 소개

- ㈜지니언스 FACT



04 회사 소개

- 주요 고객사 현황

Thank you!