



# Genian NAC v5.0 제품소개서

---

지니언스



# 목 차

- 
- 개요
  - Genian NAC 제품소개
  - 별첨
-

# Part1, 개요



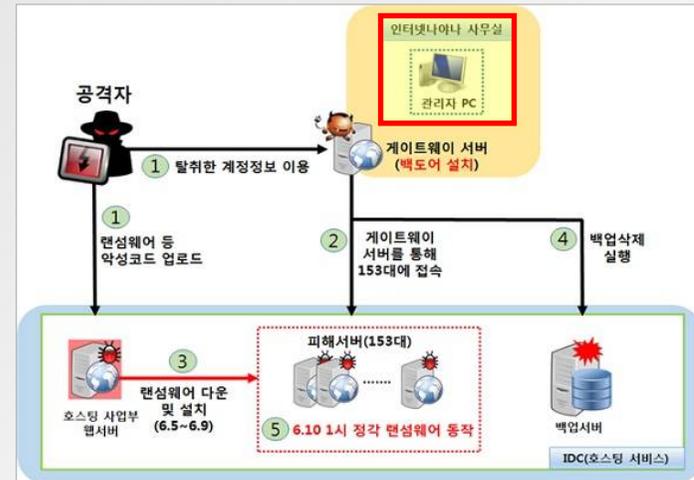
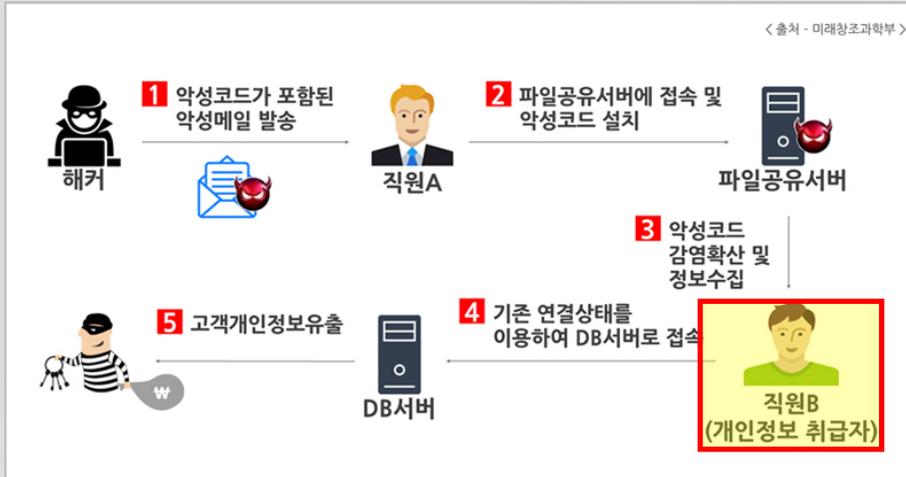
# 지속적인 내부 기술유출/보안 사고

## 전통적인 방법의 기술유출과 지능적인 해킹

### 세 가지 방법의 전통적인 기술유출

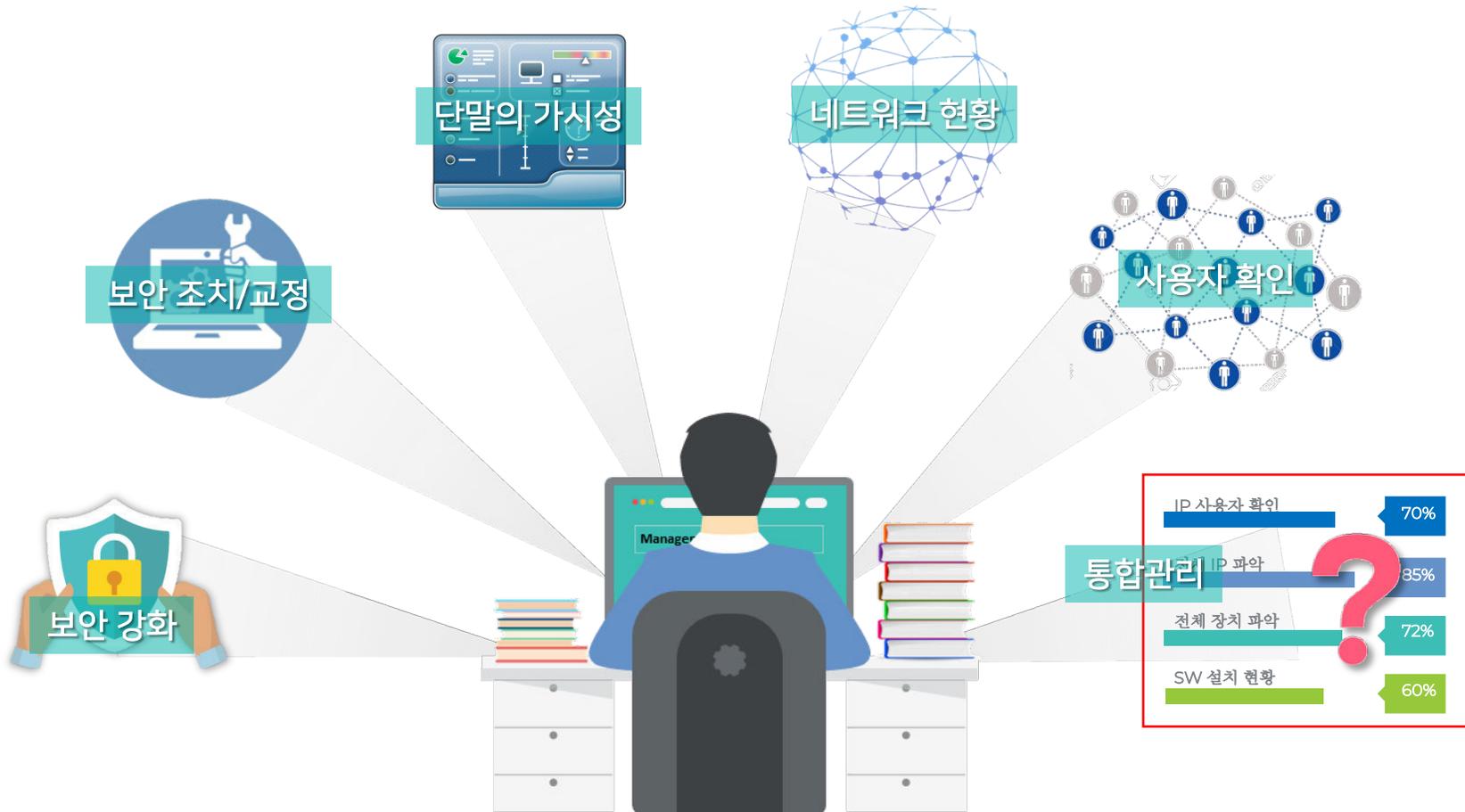
1. 기업 내부 직원과 결탁하거나 인가된 제삼자 위탁업무를 빌미로 기업에 접근해 저장 매체(USB Memory, Web Hard, CD 등)를 통해 불법적으로 기술을 빼가는 행위
2. 기업의 핵심 인력에 높은 수준의 경제적 보상책(현 급여의 5배 이상 지급 등)을 미끼로 유인, 정보 획득
3. 합법을 가장한 M&A 방법을 통해 핵심 기술 유출

APT 공격의 주 목적은 정보 탈취 및 시스템 장악으로 시스템 접속 권한이 있는 관리자 PC가 주요 표적이 되고 있다



# 관리자의 고민

지속적인 보안 사고로 인한 관리자의 역할 증가

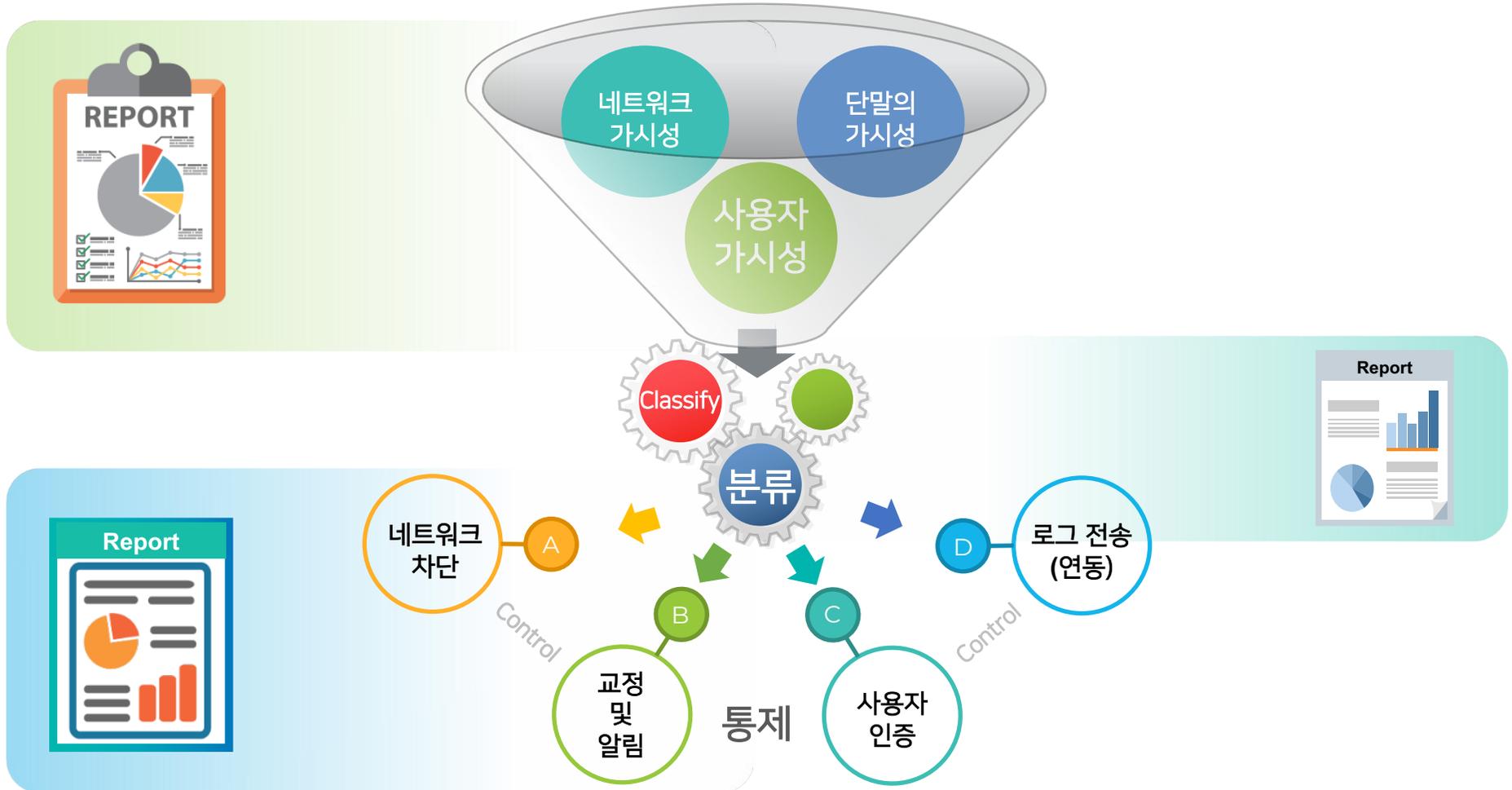


Part2,  
Genian NAC  
제품소개

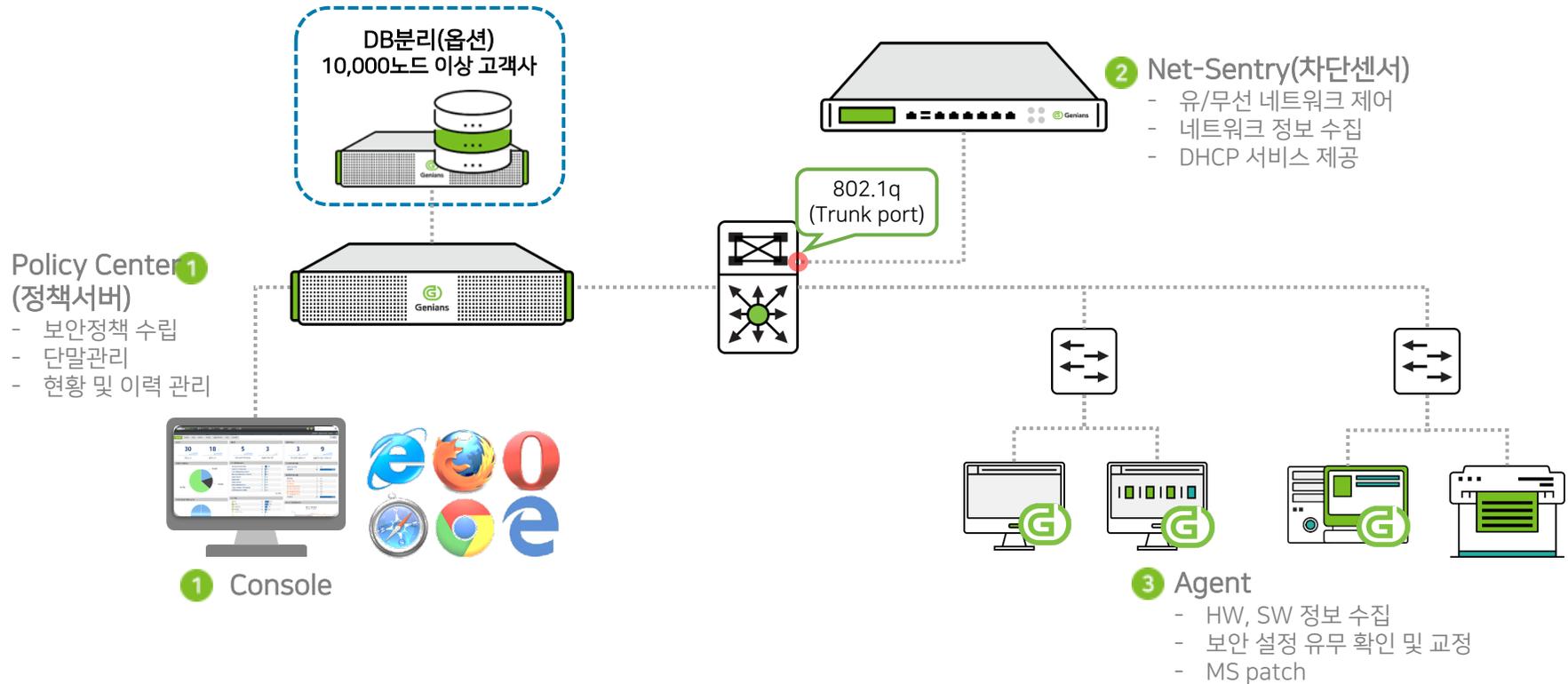


# 관리 틀을 넘어선 필수 인프라 NAC

접근제어의 필수 요소인 다양한 가시성을 통한 분류와 통제



# NAC 구성 (1/2)



## 1 정책 관리센터 & 관리콘솔 (Policy Center & Console)

유무선 네트워크를 통합 관리하고 내부 보안을 강화할 수 있도록 지원

## 2 센서(Net-Sentry)

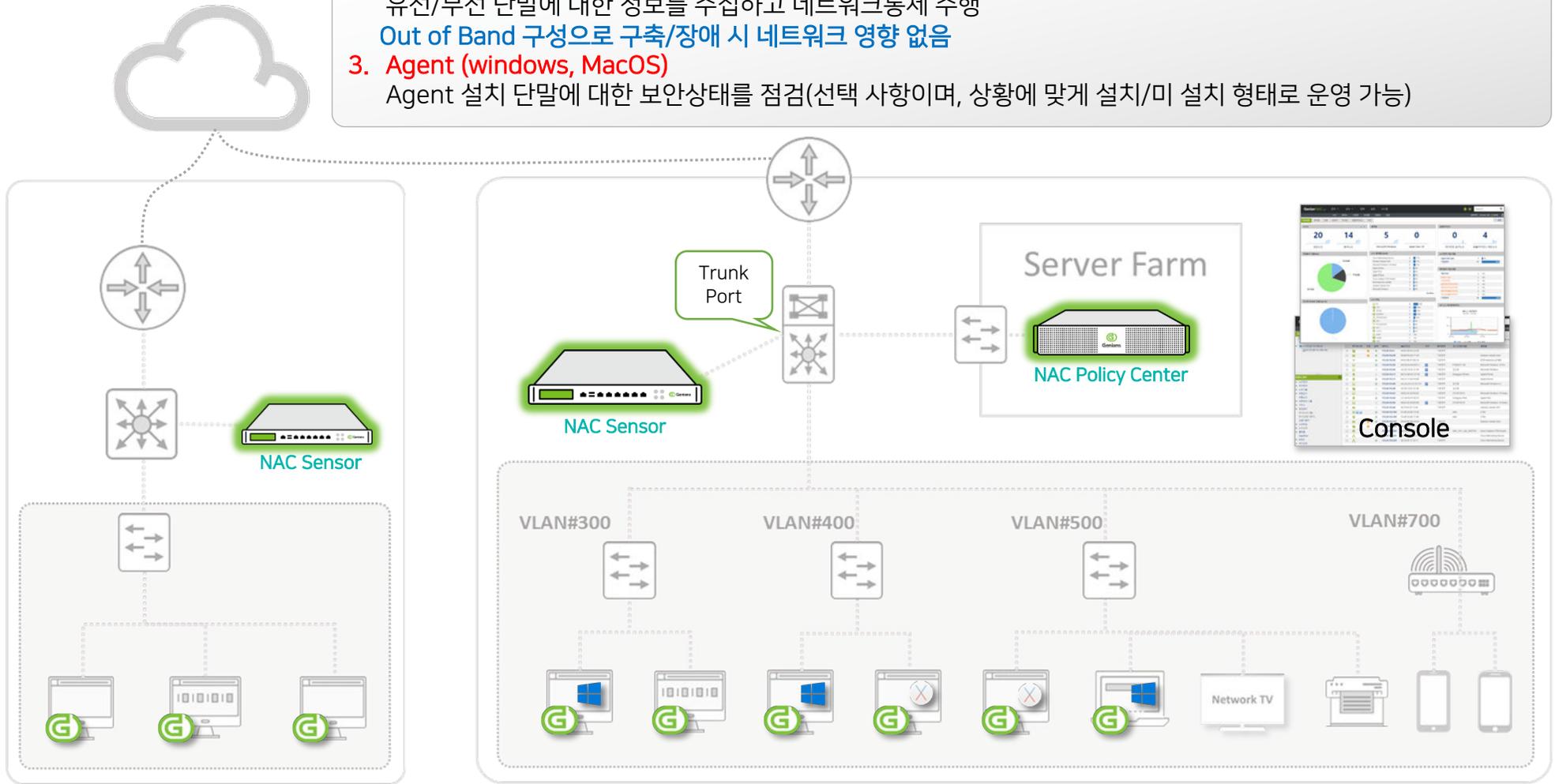
유무선 단말에 대한 정보를 수집하고 강력한 통제 수행

## 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)

# NAC 구성 (2/2)

1. **Policy Center & Console (정책서버)**  
네트워크의 가시성 제공과 정책관리, 로그 검색 등의 역할 수행
2. **NAC Sensor(Net-Sentry)**  
유선/무선 단말에 대한 정보를 수집하고 네트워크통제 수행  
Out of Band 구성으로 구축/장애 시 네트워크 영향 없음
3. **Agent (windows, MacOS)**  
Agent 설치 단말에 대한 보안상태를 점검(선택 사항이며, 상황에 맞게 설치/미 설치 형태로 운영 가능)



# 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							
NT AG SS	동작	22%	인증사용자	최근 사용자인증			172.29.50.158	E4:70:B8:EE:5B:33	50.0 연구소IP대역	Microsoft Windows 10 Home x64	F) E		DESKTOP-9KISQBM	Intel Corporate	
	동작	16%	황	2018-04-05 15:29:09			172.29.20.78	00:E0:4C:36:06:99	S-172.29.20.4	Microsoft Windows 10 Home x64	F)		DESKTOP-9KISQBM	REALTEK SEMICONDUCTOR CORP.	
	동작	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	F) E		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:DB	50.0 연구소IP대역	Samsung GALAXY S6 Phone	F)	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	F)	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	F)		KEVIN	Hon Hai Precision Ind. Co.,Ltd.	
	동작	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	F)	2018-04-05 15:03:30	HKHAN	REALTEK SEMICONDUCTOR CORP.	
	동작	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	F)		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	F)		Playdesignin	Apple, Inc.	
	동작	29%	최	2018-04-02 08:53:49			172.29.126.61	00:E0:4C:69:01:11	126.0(이상준 책임)	Microsoft Windows 10 Home x64	F)		JUNSKU-NOTEBOOK	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	F)	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	F)		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	F)	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 서버실)	Apple MacBook Pro	F)	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	F)		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	F)		YSJIN-WIN10	Micro-Star INT'L 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	F)	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	F)		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	F)		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	F)		COM-PC	GIGA-BYTE TECHNOLOGY CO.,LTD.	
	동작	85%	장	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	F)		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	F)	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	F)	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	F)		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	F)		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	F) E		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	F)	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	F)	2018-04-05 10:56:51	DESKTOP-YIHO25	Dell Inc.	
	동작	15%	이	2018-04-05 09:55:04			172.29.50.237	7C:01:91:8B:7A:45	50.0 연구소IP대역	Apple Device	F)		yih025-i6S	Apple, Inc.	
	동작	25%	이	2018-04-04 15:59:32			172.29.50.238	54:26:96:CE:A0:07	50.0 연구소IP대역	Apple MacBook Pro	F)	2018-04-05 14:56:55	MACBOOKPRO-A007	Apple, Inc.	
	동작	0%	이	2018-04-04 15:42:17	172.29.50.6	1	172.29.100.131	44:00:10:E7:93:AE	100.4(12층 서버실)	Apple iPhone	F)	2018-03-29 17:42:47	mars-iPhone	Apple, Inc.	
	동작	29%	이	2018-04-04 15:42:17	172.29.50.6	1	172.29.50.203	44:00:10:E7:93:AE	50.0 연구소IP대역	Apple iPhone	F)		mars-iPhone	Apple, Inc.	
	동작	1%	이	2018-04-04 10:45:57			172.29.128.81	00:60:6E:B3:F6:39	128.0(이재철 팀장)	Microsoft Windows 10 Home	F) E	2018-04-04 11:02:40	이종우	DAVICOM SEMICONDUCTOR, INC.	

# 가시성 (2/3)

## PC 내의 다양한 정보 제공

기본정보
장비정보

장비명: MSI 노트북 | 장비 ID: 39a3f1ce-c260-1037-0001-d1c2ba849c1

장비설명: 신상형 업무용 노트북

장비수명주기 관리: 2018-01-03 | 구입처: 구매처에서 입력 | 구매일: 2021-03-01

내용연수 시작일: 2018-03-01 | 내용연수 종료일: 2021-03-01

발행번호: 123456789 | 구입가격: 1,200,000

책임자: 김관희 | 책임부서: 구매부

제조사: 마이크로소프트 | CPU: Intel(R) Core(TM) i7-4720HQ CPU @ 2.60GHz | CPU 제조사: Intel Corporation | 리버전: 198339

메모리 정보: 전체 15.92 GB | 사용 2.86 GB | % 사용 18%

장치명	유형	변환명	공용번호	파일시스템	용량	사용된 용량	% 사용
C:	고정드라이브	/TOSHIBA THNSNJ256G8NU	15GSI00VTNMY	NTFS	227.26 GB	209.21 GB	92%
D: (차트리스드)	고정드라이브	/LITEON CV1-48128	002543120296	NTFS	119.24 GB	71.91 GB	60%
E: (드라이브D)	고정드라이브	/TOSHIBA THNSNJ256G8NU	15GSI00VTNMY	NTFS	10 GB	9.38 GB	94%

운영체제 정보: 운영체제명: Microsoft Windows 10 Professional x64 | 버전: 10.0.16299 | 서비스팩: KB4011695 | 로버전: 10.0.16299.0 | 언어: Korean | 사용자: z26d

인증정보: 도메인: FOREST-126 | 도메인: WORKGROUP | 제품 키: 2017-10-18 11:53:31 | 설치일: 2017-10-18 11:53:31 | 방화벽: 사용자 | 자동 업데이트: 6 일, 22 시간, 57 분 | 예약 작업: 사용자 | 원격 데스크톱: 허용됨

인터페이스 정보: OS: Windows 10 Pro 16299 (Windows 10 Pro 6.3) | NetBIOS computer name: FOREST-126 | Workgroup: WORKGROUP | System time: 2018-03-23 14:03:42 | 2018-04-02 08:41:00

기본정보
시스템정보

마이크로소프트 정보: 마이크로소프트 제조사: Microsoft International Co., Ltd. | CPU: Intel(R) Core(TM) i7-4720HQ CPU @ 2.60GHz | CPU 제조사: Intel Corporation | 리버전: 198339

메모리 정보: 전체 15.92 GB | 사용 2.86 GB | % 사용 18%

차량 장치 정보: 장치명, 유형, 변환명, 공용번호, 파일시스템, 용량, 사용된 용량, % 사용

운영체제 정보: 운영체제명, 버전, 서비스팩, 로버전, 언어, 사용자, 조직

인증정보: 도메인, 제품 키, 설치일, 방화벽, 자동 업데이트, 예약 작업, 원격 데스크톱

인터페이스 정보: OS, NetBIOS computer name, Workgroup, System time

기본정보
네트워크정보

트래픽 정보 (프로토콜): 프로토콜, 전체, Output

트래픽 정보 (목적지): 목적지주소, 전체, Outgoing, Incoming, 업데이트시간

접속된 AP 목록: SSID, MAC, 암호화방식, 상태, 신호 강도, 채널, 등록시간, 프로토콜, 등록상태, BSSID

TCP 세션 정보 (향상된/고대안): 세션 상태: CLOSED, ESTABLISHED, CLOSE\_WAIT, TIME\_WAIT, SYN\_SENT

접속된 서비스 목록: 구분, 정보, 등록시간, 업데이트시간, 동작

SMB 공유: OS: Windows 10 Pro 16299 (Windows 10 Pro 6.3) | NetBIOS computer name: FOREST-126 | Workgroup: WORKGROUP | System time: 2018-03-23 14:03:42 | 2018-04-02 08:41:00

방화벽 정보: 프로토콜, 포트, 프로세스명, 네트워크 서비스, 상태, 등록시간

기본정보
소프트웨어정보

특성 정보: Windows Defender | 제품 버전: 1.263.1913.0 | 현재 버전: 2018-04-02 05:55:37 | 실시간 검사: 동작

소프트웨어 정보: 프로그램명, 버전, 경로, 설치일자, 등록시간

프로그램명	버전	경로	설치일자	등록시간
Adobe Acrobat Reader DC - Korean	18.011.20038	C:\Program Files (x86)\Adobe\Acrobat Reader DC\	20180226	2018-03-29 08:50:44
Adobe Creative Cloud	4.4.1.206			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	1.3.25.1015	C:\Program Files\AhnLab\Safe Transaction	20180125	2018-03-29 08:50:44
AmySignMPC 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
AudPlayer	1.9.17.0			2018-03-29 08:50:44
BitTorrent	7.10.0.43917	C:\Users\z26d\AppData\Local\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

작업 중인 Windows 업데이트 목록: Default Windows Update (온라인) | 최근 추종 결과

업데이트명	분류	릴리스	업데이트 상태	설치/승인 상태	업데이트 시간
2018-03-x64 기반 시스템용 Windows 10 Version 1709의 Adobe Flash Player 보안 업데이트(KD4088785)	보안 업데이트	2018-03-13	완료	미승인	2018-03-29 10:27:06
2018-03-x64 기반 시스템용 Windows 10 Version 1709에 대한 수직 업데이트(KB4088776)	보안 업데이트	2018-03-13	완료	미승인	2018-03-29 10:27:06
Microsoft Word 2013용 보안 업데이트(KB4016695) 32비트 버전	보안 업데이트	2018-03-13	완료	미승인	2018-03-29 10:27:06
Microsoft Excel 2013용 보안 업데이트(KB4016291) 32비트 버전	보안 업데이트	2018-03-13	완료	미승인	2018-03-29 10:27:06
Windows 악성 소프트웨어 제거 도구 x64 - 2018년 3월(KB989830)	보안 업데이트	2018-03-13	완료	미승인	2018-03-29 10:27:06
Skype for Business 2015용 업데이트(KB4018290) 32비트 버전	응용 업데이트	2018-03-06	완료	미승인	2018-03-29 10:27:06
Microsoft Office 2013용 업데이트(KB4018291) 32비트 버전	응용 업데이트	2018-03-06	완료	미승인	2018-03-29 10:27:06
Microsoft Office 2013용 업데이트(KB4011552) 32비트 버전	응용 업데이트	2018-03-06	완료	미승인	2018-03-29 10:27:06
Microsoft Project 2013용 업데이트(KB4018292) 32비트 버전	응용 업데이트	2018-03-06	완료	미승인	2018-03-29 10:27:06
Microsoft Office 2013용 업데이트(KB3172471) 32비트 버전	응용 업데이트	2018-03-06	완료	미승인	2018-03-29 10:27:06
Microsoft Office 2013용 보안 업데이트(KB3172458) 32비트 버전	보안 업데이트	2018-02-13	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

기본정보
이력관리

이력관리: 시간, 로그종류, 로그ID, 관리자명, IP, MAC, 사용자ID, 사용자명, 부서명, 설명

2018-03-30 16:33:39	알림	시스템정보	172.28.112.100	172.28.112.56	D8:CB:8A:84:D9:C1				모니터 정보 추가 감지됨. SERIALNUMBER=000000000000
2018-03-30 16:33:31	알림	아이콘트랜	172.28.112.100	172.28.112.56	D8:CB:8A:84:D9:C1				아이콘트랜션 실패. RESULT=FAIL. ACTION=백신프로그램 존재, TYPE=NEW
2018-03-30 10:37:23	알림	불정변경	172.28.112.100	172.28.112.56	D8:CB:8A:84:D9:C1				장비의 속성이 변경됨. ADMIN=forest, ADMIN_IP=172.29.112.56
2018-03-30 10:01:23	알림	시스템정보	172.28.112.100	172.28.112.56	D8:CB:8A:84:D9:C1				모니터 정보 삭제 감지됨. SERIALNUMBER=000000000000
2018-03-30 10:01:23	알림	시스템정보	172.28.112.100	172.28.112.56	D8:CB:8A:84:D9:C1				소프트웨어목록 추가 감지됨. NAME=Dropbox, VERSION=46.4.05, PATH=C:\P
2018-03-30 10:01:23	알림	시스템정보	172.28.112.100	172.28.112.56	D8:CB:8A:84:D9:C1				소프트웨어목록 삭제 감지됨. NAME=Dropbox, VERSION=46.4.05, PATH=C:\P
2018-03-29 09:42:50	알림	불정변경	172.28.112.100	172.28.112.56	D8:CB:8A:84:D9:C1				장비의 속성이 변경됨. ADMIN=forest, ADMIN_IP=172.29.112.56
2018-03-29 08:50:56	알림	시스템정보	172.28.112.100	172.28.112.56	D8:CB:8A:84:D9:C1				모니터 정보 추가 감지됨. SERIALNUMBER=unknown serial [BOE5E3]
2018-03-29 08:50:56	알림	시스템정보	172.28.112.100	172.28.112.56	D8:CB:8A:84:D9:C1				모니터 정보 추가 감지됨. SERIALNUMBER=000000000000
2018-03-29 08:50:56	알림	시스템정보	172.28.112.100	172.28.112.56	D8:CB:8A:84:D9:C1				프린터 정보 추가 감지됨. PRINTERNAME=\\172.29.100.160\Canon MB2300 ser
2018-03-29 08:50:56	알림	시스템정보	172.28.112.100	172.28.112.56	D8:CB:8A:84:D9:C1				프린터 정보 추가 감지됨. PRINTERNAME=(128)\Canon iR-ADR C5300 C5305 C
2018-03-29 08:50:56	알림	시스템정보	172.28.112.100	172.28.112.56	D8:CB:8A:84:D9:C1				프린터 정보 추가 감지됨. PRINTERNAME=098 캐논복합기

# 가시성 (3/3)

## Dashboard 를 통한 다양한 통계, 상태 등의 현황 파악 용이

The dashboard provides a comprehensive overview of the network environment. Key sections include:

- System Overview:** Displays overall statistics such as 1,355 total nodes, 287 PCs, 77 mobile devices, and 13 IP-managed devices.
- Device Management:** Lists various devices categorized by OS (e.g., Windows, Linux, macOS) and manufacturer (e.g., Cisco, HP, Dell).
- Network Status:** Shows connection status for different network segments like PC, WAP, and Mobile.
- Device Details:** A detailed view of a selected device (e.g., IP 172.28.196.132) showing its IP management status, MAC management status, and associated user information.
- Alerts and Notifications:** A section for managing alerts and notifications.

# 분류 (1/2)

## 다양한 분류 조건 제공(Dynamic Classification)

### 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

### 그룹 조건 sample

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 (2/2)

## 분류된 정보를 볼 수 있는 통계화면 제공

### 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%

### 노드 타입

타입	수량	비율
PC	288	21%
기타	258	19%
보안장비	232	17%
서버	121	9%
VOIP	112	8%
네트워크장비	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%

### IP관리 정책현황

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

정책명	노드 수
IP 차단	8
IP 허용	1323
IP 허용 - 충돌보호(지정 MAC)	1
IP 허용 - 충돌보호(지정 MAC) - 단일 MAC	1
IP 허용 - 충돌보호(지정 MAC) - 다중 MAC	0
IP 허용 - 충돌보호(지정 MAC) - Unknown MAC	0
MAC 차단	0
MAC 허용	955
MAC 허용 - 변경금지(모든 IP대역)	1
MAC 허용 - 변경금지(모든 IP대역) - 단일 IP	0
MAC 허용 - 변경금지(모든 IP대역) - 다중 IP	0
MAC 허용 - 변경금지(지정 IP대역)	0
MAC 허용 - 변경금지(지정 IP대역) - 단일 IP	0
MAC 허용 - 변경금지(지정 IP대역) - 다중 IP	0
IP사용시간 제한	0

### 제어정책 적용 현황

정책명	노드 수	비율
HDH_netctrl_test	0	0%
예외허용	1012	77%
다중미동작 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%
패시상태불만족차단	0	0%
백신상태불만족차단	0	0%
기본정책	241	18%

### 등록현황

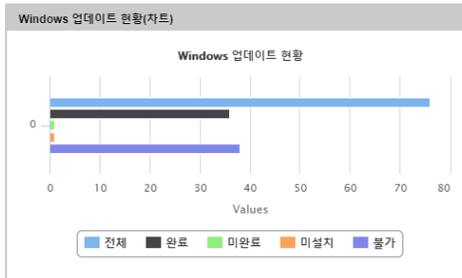
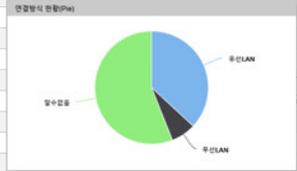
기간	노드	장비	에이전트
직전 로그인이후	22	2	1
오늘	51	11	2
1일이상	157	43	4
7일이상	328	197	10
30일이상	845	684	64
수신안됨	0	0	0

### 노드그룹 정책적용 현황

ID	노드수
모든노드	1381
예외노드	725
(예외) 신성한 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	
패시상태불만족노드	
(예외) 임시 예외노드	
Defender 모니터링 그룹	
PC	
(그룹) 경영관리실	
(그룹) 커뮤니케이션실	5
백신 미준제	4
(그룹) 신규사업FTT	3
Insights테스트(shlee)	3
(예외) 발드서버	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
	8
	7
	7
	7
	6
	4
	4
	4
	4
	3
	2
	2
	2



### 노드 태그

HDH테스트	0	0%
THREAT	0	0%
고위험	1	0%
관리자	0	0%
네트워크차단	0	0%
악성코드차단	0	0%
에이전트 설치(예외)	7	1%
임시예외	1	0%
장치제어(예외)	1	0%
중위험	1	0%

## 차단, 알림, 교정의 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, snmptrap)

The screenshot shows the Genian NAC v3.0 interface. At the top, there are navigation tabs: 관리, 감사, 정책, 설정, 시스템. Below is a '로그' (Log) section with a bar chart showing log activity from 03/26 to 04/01. Below the chart is a table of log entries with columns: 시간, 로그종류, 로그ID, 관리자비명, IP, MAC, 사용자ID, 사용자명, 부서명, 설명. Several entries are highlighted in yellow, including a warning (경고) for 'GENIAN장비' and several '알림' (Info) entries for '데이터베이스 접속실패' and '시스템관리'.

### 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 tilde를 사용합니다. 단독 단어의 끝에 ~ 표시하십시오. 예를 들어, "roam"과 스펠링이 유사한 단어를 검색하기 위해 fuzzy 검색을 사용합니다.

현재 검색조건을 검색기간 [1주] 으로 검색필터에 저장합니다.

이름:

설명:

관심필터:  검색필터를 로그 트리 및 로그모니터에 표시합니다.

출력컬럼: 

사용가능	선택
<input type="checkbox"/>	<input type="checkbox"/>

\* 메시징내에 사용가능한 매크로 도움말

알람전송:  해당 로그 발생시 관리자에게 알람을 전송합니다.

SYSLOG 전송:  해당 로그 발생시 SYSLOG서버로 전송합니다.

SNMP Trap 전송:  해당 로그 발생시 SNMP서버로 SNMP Trap을 전송합니다.

Webhook:  해당 로그 발생시 설정한 URL에이자를 호출합니다.

태그:

생성    목록

# 리포트 (2/2)

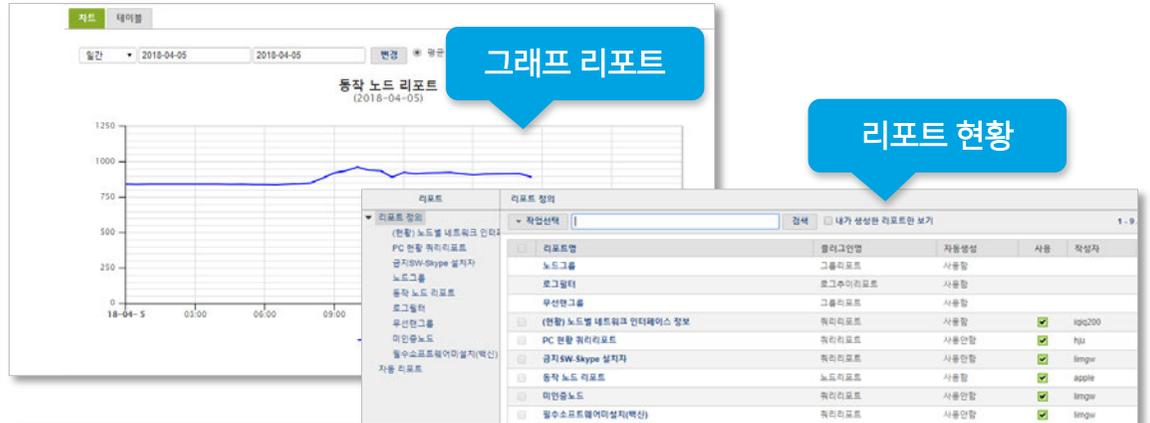
## 노드, 쿼리, 로그 Report 제공

이름	오늘	전일	전주	전월	변동폭		
					전일비	전주비	전월비
에이전트미동작노드	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) 신성한 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
패자상태불안측노드	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
회면보조기 미설정	1	5	5	0	▼2	▼2	▼3
(그룹) 해외사업부	2	1	1	2	▲1	▲1	0
(예외) 발드서버	2	1	1	1	▲1	▲1	▲1
Apple Mac OS	37	38	37	38	▼1	0	▼1
Insights개발(\\'1)	10	11	10	10	▼1	0	0

증감 추이 리포트

IP	MAC	인증사용자	부서	관리센터	CPU	전체메모리	사용메모리	메모리사용률	
172.172.158	E4:70:B8:E8:58:33	관리	인력사업부	S-172	Intel(R) Core(TM) i3-7100U CPU @ 2.40GHz	8217872	2010740	24%	
172.172.178	00:ED:4C:36:06:99	관리	인력사업부	S-172	Intel(R) Core(TM) i3-7100U CPU @ 2.40GHz	8217872	2010740	24%	
172.172.228	DC:0B:34:B9:A6:C9	관리	MAC 개발실	S-172	228				
172.172.229	E8:3A:12:1C:08:DB	관리	신규사업TFT	S-172	229				
172.172.219	80:E6:50:0F:5D:88	관리	인력사업부	S-172	158	Intel(R) Core(TM) i3-3220 CPU @ 3.30GHz	3849584	1677780	48%
172.172.41	D0:27:88:D9:3C:8E	관리	인력사업부	S-172	158	Intel(R) Core(TM) i7-8550U CPU @ 1.80GHz	16640366	7138712	43%
172.172.42	00:ED:4C:39:48:43	관리	인력사업부	S-172	228	Intel(R) Core(TM) i5-4210U CPU @ 1.70GHz	8294176	2094956	25%
172.172.58	D0:59:99:81:D3:70	관리	인력사업부	S-172	229	Intel(R) Core(TM) i7-8700K CPU @ 4.00GHz	16440628	1441332	9%
172.172.189	D0:2B:20:89:DA:2B	관리	인력사업부	S-172	229	Intel(R) Core(TM) i5-4210U CPU @ 1.70GHz	8294176	2094956	25%
172.172.161	00:ED:4C:69:01:11	관리	인력사업부	S-172	5.61	Intel(R) Core(TM) i7-8550U CPU @ 1.80GHz	16640366	7138712	43%
172.172.129	84:86:78:77:AA:06	관리	Endpoint 개발실	S-172	9.29	Intel(R) Core(TM) i5-3337U CPU @ 1.80GHz	8001052	1843548	23%
172.172.180	40:8D:5C:70:F7:22	관리	Endpoint 개발실	S-172	180	Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz	16638244	10133172	61%
172.172.199	6C:4D:73:DA:29:09	관리	Insights 개발실	S-172	199				
172.172.234	AC:BC:32:D6:1D:43	관리	Insights 개발실	S-172	234				
172.172.201	8C:89:A5:E2:19:7A	관리	Insights 개발실	S-172	201	Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz	16708180	13090706	78%
172.172.200	80:EA:9E:E0:05:08	관리	MAC 개발실	S-172	200				
172.172.90	1C:18:0D:4F:35:34	관리	감정관리실	S-172	90	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz	16667544	3994692	24%
172.172.88	ED:D5:5E:59:BA:94	관리	감정관리실	S-172	88	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz	16662220	5189904	31%
172.172.204	49:8D:5C:FC:C8:4F	관리	감정관리실	S-172	204	Intel(R) Core(TM) i7-6700K CPU @ 4.00GHz	16654776	3128368	19%
172.172.20	FC:AA:1A:ED:D2	관리	감정관리실	S-172	20	Intel(R) Core(TM) i3-4160 CPU @ 3.60GHz	16652816	6833784	41%

쿼리 리포트 (관리자 지정)



파일명	생성일자
(현황) 노드별 네트워크 인터페이스 정보-180405-100001454.xls	2018-04-05 10:00:01
(현황) 노드별 네트워크 인터페이스 정보-180404-100001400.xls	2018-04-04 10:00:01
(현황) 노드별 네트워크 인터페이스 정보-180403-100001400.xls	2018-04-03 10:00:01
(현황) 노드별 네트워크 인터페이스 정보-180402-100001400.xls	2018-04-02 10:00:01
(현황) 노드별 네트워크 인터페이스 정보-180401-100001122.xls	2018-04-01 10:00:01

스케줄 가능

엑셀 변환

cmd	NI_DEVICE	IP	MAC	ADDR	NETMASK
2 0d80d572-8028-1035-8018-4446a5620b3f	Wi-Fi	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
2 0d80d572-8028-1035-8018-4446a5620b3f	이더넷	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
4 0e90c48-8035-1037-819a-0000c4504024	10 Ethernet adapter	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
4 0e90c48-8035-1037-819a-0000c4504024	Wi-Fi	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
4 0e90c48-8035-1037-819a-0000c4504024	로컬 영역 연결* 12	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
4 0e90c48-8035-1037-819a-0000c4504024	이더넷 2	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
2 0002306a-b21e-1001-8002-0000c6d6b963	Wi-Fi	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
2 0002306a-b21e-1001-8002-0000c6d6b963	이더넷 7	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
3 13c37a58-9b0c-1036-8066-10a4a7d7038a2	로컬 영역 연결* 7	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
3 13c37a58-9b0c-1036-8066-10a4a7d7038a2	로컬 영역 연결* 2	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
3 13c37a58-9b0c-1036-8066-10a4a7d7038a2	무선랜카드 연결	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
4 18130384-8353-1035-803a-4006d5c79685	VPN - VPN Client	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
4 18130384-8353-1035-803a-4006d5c79685	로컬 영역 연결* 1	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
4 18130384-8353-1035-803a-4006d5c79685	이더넷	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
4 18130384-8353-1035-803a-4006d5c79685	이더넷 4	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
3 1956a60c-2551-1037-8366-1807b0cc0f04	Wi-Fi	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
3 1956a60c-2551-1037-8366-1807b0cc0f04	로컬 영역 연결* 12	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
3 1956a60c-2551-1037-8366-1807b0cc0f04	이더넷	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
4 20c8b0d4-04a4-1037-807a-980389145191	Wi-Fi	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
4 20c8b0d4-04a4-1037-807a-980389145191	이더넷	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
4 20c8b0d4-04a4-1037-807a-980389145191	이더넷 2	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
4 20c8b0d4-04a4-1037-807a-980389145191	이더넷 3	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
2 209610b-8e6b-1037-827a-0a0d17022631	Wi-Fi	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
2 209610b-8e6b-1037-827a-0a0d17022631	이더넷 8	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
2 209610b-8e6b-1037-827a-0a0d17022631	이더넷 6	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
2 20bae02-64c4-1036-8051-0000c4794843	Wi-Fi	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
3 3546a828-9719-1036-8059-001062a9c78	Wi-Fi	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
3 3546a828-9719-1036-8059-001062a9c78	이더넷 2	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
3 3546a828-9719-1036-8059-001062a9c78	이더넷	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
3 3546a828-9719-1036-8059-001062a9c78	이더넷 2	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
3 3546a828-9719-1036-8059-001062a9c78	이더넷 2	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
3 367c789-8376-1035-8037-1867b0c5a622	Wi-Fi	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
3 367c789-8376-1035-8037-1867b0c5a622	로컬 영역 연결* 14	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
3 367c789-8376-1035-8037-1867b0c5a622	이더넷	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0
3 382a92c2-468b-1037-8012-1867b0431360	Wi-Fi	172.172.158	84:86:78:77:AA:06	172.172.158.255	255.255.255.0

# Genian NAC 기능 요약

## 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, Wi-Fi, 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, 공유폴더 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

Windows



## 단말 플랫폼 인텔리전스(DPI)



SOLUTIONS ▾

GENIAN NAC ▾

RESOURCES ▾

COMPANY ▾ 🔍

TRIAL & BUY

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

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



## Cisco Catalyst 2960X-24TS

Platform Information <http://www.router-switch.com/ws-c2960x-24ts-ll>

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.

#### 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

# 제품 특징점

## 단말에서 발생하는 악성코드를 탐지

**Genian NAC v5.0** 관리 | 감사 | 정책 | 설정 | 시스템

지니안 NAC | 노드 | IP주소 | 스위치 | 무선랜 | 사용자 | 신청

노드: 172.29.50.93 / D0:27:88:D5:98:0C

노드목록 | 노드그룹 지정/해제 | 인스턴트메시지 전송 | 접속인증페이지(CWP) 조회 | 노드대상 작업지시

기본정보 | 장비정보 | 시스템정보 | 네트워크정보 | 소프트웨어정보 | 운영체제 업데이트 정보 | 이력관리 | IP관리 | 정책 | 정책현

감지 시각	파일명	위협종류	위험도	신뢰도	파일크기	서명자 이름	생성시각
2019-02-12 02:17:20	malware.exe	Trojan	●	87%	481,280 bytes		2019-02-12

**Malware 파일**

감지 시각	2019-02-12 02:17:20
파일명	malware.exe
경로	C:\_temp2\malware.exe
위협종류	Trojan
위험도	●
신뢰도	87%
파일크기	481,280 bytes
서명자 이름	
ISSUER	
MD5	059BB09924B0D8CB7A8CFFB72FD08B03
SHA1	87A02BE494BC914211D91A45A9CCBF4D47238566
SHA256	0ABB52B3E0C08D5E3713747746B019692A05C5AB8783FD99B1300F11EA59B1C9
생성시각	2019-02-12 02:14:19
수정시각	2019-02-08 06:49:34

**Malware 탐지 현황**

파일명	위협종류	위험도	신뢰도	파일크기	수량
malware.exe	Trojan	●	87%	481,280 bytes	2
malware.exe	Trojan	●	87%	481,280 bytes	3

**Malware 탐지를 위한 정보 수집 동의**

비판 1:17 5610  
 설명 Insights ECO 시스템과 연동하여 단말에서 발생하는 악성코드를 감지합니다.  
 파일명 MalwareDetector.cab  
 동작방식 항상 실행

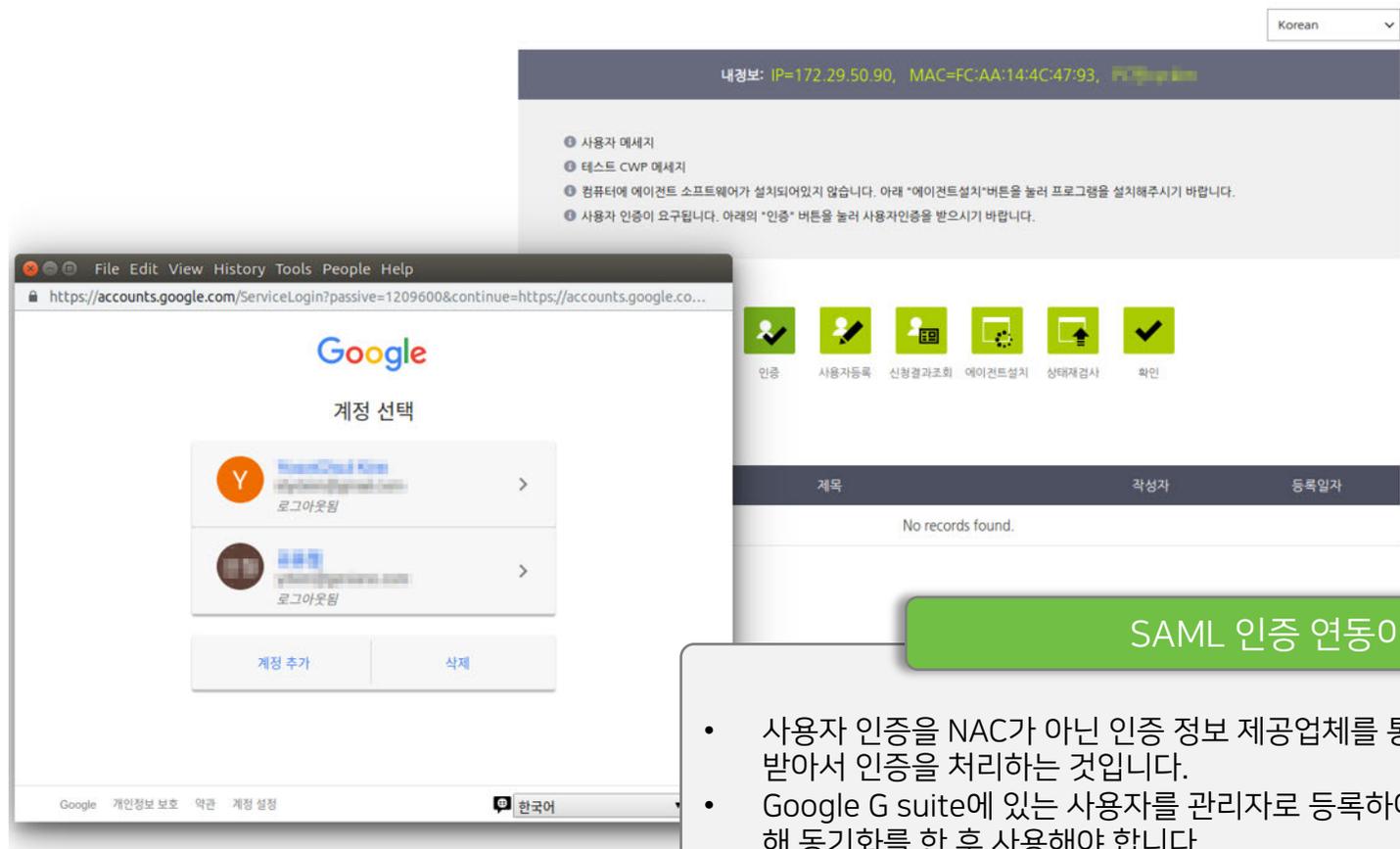
핵심 플러그인은 NAC 사용자에게 악성코드 탐지 기능을 제공하며 개선을 위해 일의 변경될 수 있습니다.

정보수집 동의  
 플러그인을 사용하기 위해서는 정보수집에 대한 사용자 및 관리자의 동의가 필요합니다. 사용자관리자는 아래 명시된 정보의 수집, 제공, 이용에 관한 내용을 확인하고 이를 거부할 수 있습니다. 만약 거부하는 경우 해당 기능의 사용이 불가능합니다.

- 정보의 수집
  - NAC Agent가 설치 및 운영중인 단말에서 악성코드 탐지를 위하여 실행파일(EXE 등)을 대상으로 필요한 정보를 수집합니다.
  - 수집하는 정보는 악성코드 탐지를 위한 (1) 파일정보(파일명, 저서 등) (2) 관리자명정보(서명어부, 서명자 이름 및 저서 등) 또는 (3) 파일정보(실제 파일 자체) 등 이하 기능을 위하여 임의 변경될 수 있습니다.
- 정보의 제공
  - 수집된 정보는 분석을 위하여 개발사 또는 제3자에 유한한 권한을 제한한 제3자(민은 분석 기관 등)에게 제공할 수 있습니다.
  - 악성코드 탐지 및 분석을 제외한 어떠한 목적으로도 임의 제공되지 않습니다.
- 정보의 이용
  - 다양하고 고도화된 기술적 방법을 이용하여 악성코드 여부를 판단하고 그 결과를 알려드립니다.
  - 민간 결과에 대한 실시간(Real Time) 계측 및 악성코드에 대한 결과를 100% 보증하지 않습니다.
  - 유사 유행성과 관련 결과가 다를 수 있으며 최종 판단의 책임은 사용자관리자에게 있습니다.

수집제외 정보  
 %PROGRAMFILES%\AhnLabi\3IS90\update\2\update\*  
 %PROGRAMFILES%\AhnLabi\3IS90\Quarantine\*  
 %SYSTEMDRIVE%\ProgramData\ESTsoft\ALV\update\*  
 %SYSTEMDRIVE%\ProgramData\ESTsoft\ALV\Quarantine\*  
 %SYSTEMDRIVE%\ProgramData\Hour\VRIS70\Backup\*  
 %SYSTEMDRIVE%\ProgramData\Hour\VRIS70\Backup\*  
 Malware 탐지에 필요한 정보 수집에서 제외할 폴더 경로를 설정합니다.  
 \*가용공간을 사용할 수 있습니다.  
 ex) 특정인물 "%GoogleChrome\Application"

## SAML (G-Suite 인증)



The screenshot displays the Google Accounts Service Login interface. On the left, a browser window shows the '계정 선택' (Account Selection) page with two Google accounts listed. On the right, a larger window shows a progress bar with six steps: 인증 (Authentication), 사용자등록 (User Registration), 신청결과조회 (Check Application Results), 에이전트설치 (Agent Installation), 상태재검사 (Check Status), and 확인 (Confirmation). The '인증' step is marked with a checkmark. Below the progress bar, a table with columns '계목' (Category), '작성자' (Author), and '등록일자' (Registration Date) shows 'No records found.'

내정보: IP=172.29.50.90, MAC=FC:AA:14:4C:47:93, PC=...

● 사용자 예세기  
● 테스트 CWP 예세기  
● 컴퓨터에 에이전트 소프트웨어가 설치되어있지 않습니다. 아래 "에이전트설치"버튼을 눌러 프로그램을 설치해주시기 바랍니다.  
● 사용자 인증이 요구됩니다. 아래의 "인증" 버튼을 눌러 사용자인증을 받으시기 바랍니다.

계정 선택

계정 추가 삭제

인증 사용자등록 신청결과조회 에이전트설치 상태재검사 확인

계목 작성자 등록일자

No records found.

SAML 인증 연동이란?

- 사용자 인증을 NAC가 아닌 인증 정보 제공업체를 통해서 인증을 하고 그에 대한 결과를 받아서 인증을 처리하는 것입니다.
- Google G suite에 있는 사용자를 관리자로 등록하여 사용할 경우에는 정보동기화를 통해 동기화를 한 후 사용해야 합니다.

# 제품 특징점

## 다양한 DB와의 연동을 통해 NAC 에 특정 정보 자동 등록/관리

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



**사용자정보**

사용자아이디불명  
데이터를 읽어올 데이터베이스의 사용자아이디불명을 설정합니다. (RDBMS의 경우 테이블이름, LDAP의 경우 사용자 검색 Base DN, CSV인 경우는 사용하지 않음)

사용자조건문  
데이터를 읽어올 데이터베이스의 사용자아이디에 대한 쿼리 WHERE 조건문을 설정합니다. LDAP인 경우 filter사용. filter 예제: (objectClass=person)

NTAG 55	위험	동작	IP주소	MAC주소	성적	제어정책	호스트(이름)	플랫폼	인증사용자	위치	가동률
			172.29.112.4	44:8A:5B:6A:2A:95	기본정책	일건용	Geniens Genian NAC	Microsoft Windows 10 Professional x64	인용사용자	5-172.29.112.100	99%
			172.29.112.49	00:90:F8:2D:77:A9	기본정책	일건용	EFM Networks ipTIME	Microsoft Windows 10 Professional x64	인용사용자	5-172.29.112.100	100%
			172.29.112.58	84:E5:98:07:5B:C9	기본정책	일건용	Microsoft Windows 10 Professional x64	Microsoft Windows 10 Professional x64	인용사용자	5-172.29.112.100	20%
			172.29.112.56	D8:CB:8A:84:D9:C1	기본정책	일건용	FOREST-126	Microsoft Windows 10 Professional x64	인용사용자	5-172.29.112.100	2%
			172.29.112.60	AC:E0:10:61:A1:0F	기본정책	일건용	MACBOOKPRO-AA90	Apple MacBook Pro	인용사용자	5-172.29.112.100	7%
			172.29.112.67	60:F8:1D:BE:AA:90	기본정책	일건용	Samsung-Galaxy-S7	Samsung GALAXY S7 Phone	인용사용자	5-172.29.112.100	0%
			172.29.112.69	E4:FA:ED:1C:2B:27	기본정책	일건용	Donggusi-iPhone	Apple iPhone	인용사용자	5-172.29.112.100	3%
			172.29.112.73	80:CA:58:5C:CF:58	기본정책	일건용	Apple Device	Apple Device	인용사용자	5-172.29.112.100	53%
			172.29.112.75	D8:33:11:D4:F9:D6	기본정책	일건용	Microsoft Windows 8.1	Microsoft Windows 8.1	인용사용자	5-172.29.112.100	0%
			172.29.112.80	ACE0:10:61:A1:0F	기본정책	일건용	Microsoft Windows 8.1	Microsoft Windows 8.1	인용사용자	5-172.29.112.100	21%
			172.29.112.82	AA:AA:AA:CC:CC:CC	기본정책	일건용	Microsoft Windows 8.1	Microsoft Windows 8.1	인용사용자	5-172.29.112.100	21%

회사이름컬럼명  
부서ID컬럼명  
직급ID컬럼명  
전화번호컬럼명  
휴대폰컬럼명  
이메일컬럼명  
주소컬럼명  
설명컬럼명  
추가정보1컬럼명  
추가정보2컬럼명  
추가정보3컬럼명

**사용자정보**

**노드정보**

노드정보테이블명  
데이터를 읽어올 데이터베이스의 노드정보테이블명을 설정합니다. (RDBMS의 경우 테이블이름, LDAP의 경우 사용자 검색 Base DN, CSV인 경우는 사용하지 않음)

노드정보조건문  
데이터를 읽어올 데이터베이스의 노드정보테이블에 대한 쿼리 WHERE 조건문을 설정합니다. LDAP인 경우 filter사용. filter 예제: (objectClass=group)

IP주소컬럼명  
MAC주소컬럼명  
노드이름컬럼명  
노드설명컬럼명  
인증사용자ID컬럼명  
추가정보1컬럼명  
추가정보2컬럼명  
추가정보3컬럼명

노드정보

추가정보  
추가정보  
추가정보

제조일  
내용연수 시작일  
구입처  
구입가격  
책임자  
책임부서  
내용연수 만료일  
메모  
추가정보1컬럼명  
추가정보2컬럼명  
추가정보3컬럼명

**장비수명주기정보**

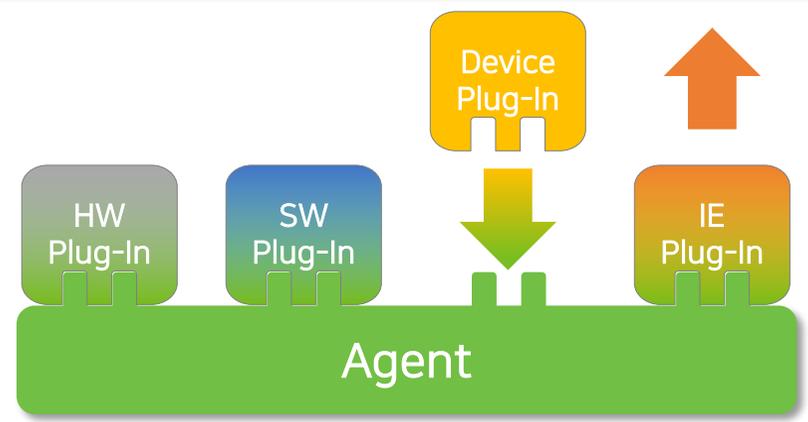
# 제품 특징점

## 사용자 PC 의 안정성을 보장하는 Agent



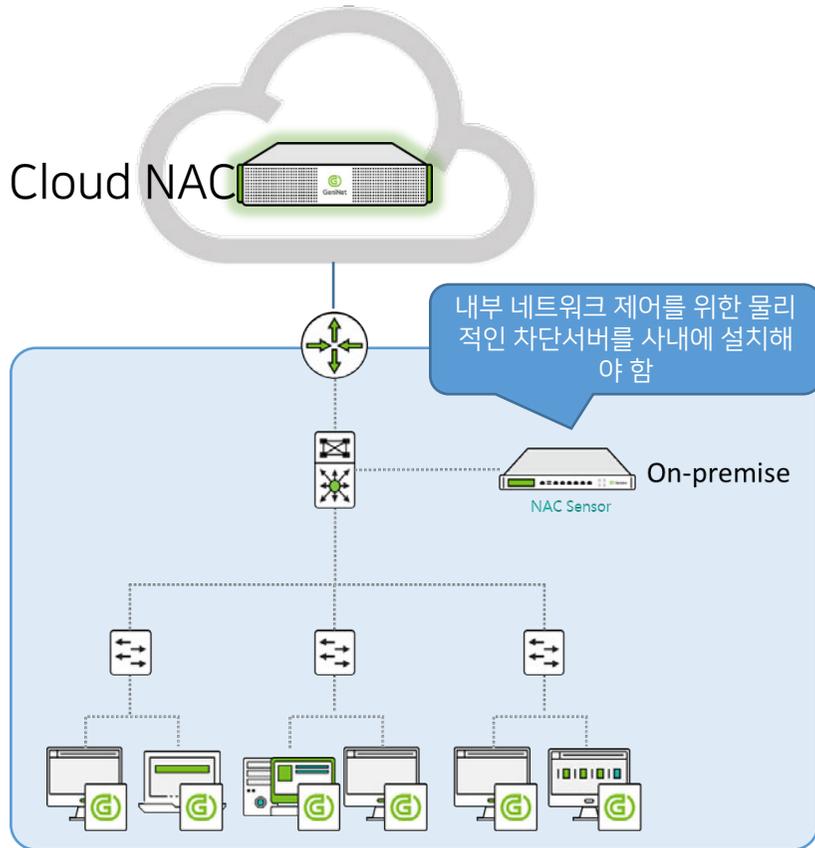
- 모든 기능 플러그인 형태로 제공하여 선택/추가 용이함
- 선택적 기능 사용으로 리소스 사용 최소화
- Non-Kernel 기반의 동작(OS 충돌 위험 거의 없음)

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



## Cloud NAC / Device Platform Intelligence

- 클라우드 서비스를 이용한 정책서버 구성(AWS)



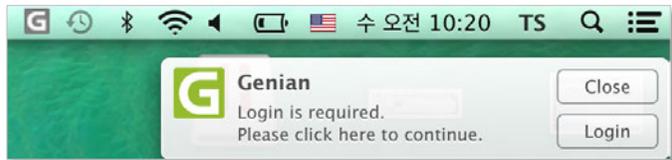
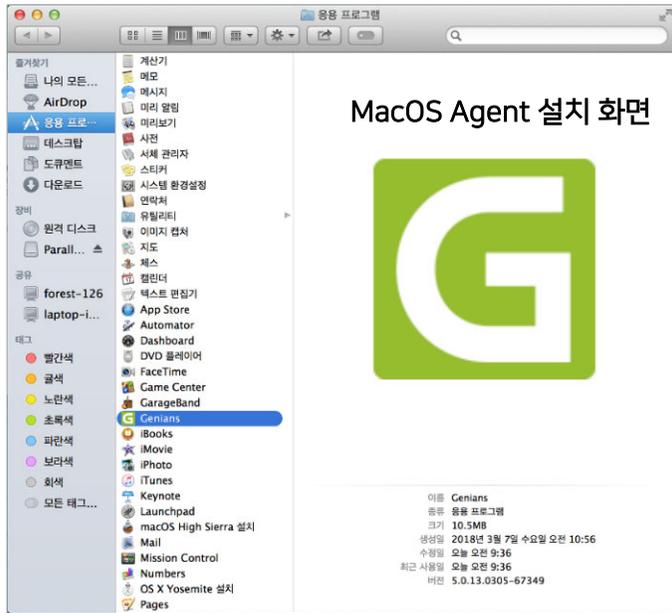
- 장치에 대한 제조사 지원 현황 제공 (홈페이지, 제조사, 판매상태 등)

IP Address	MAC Address	Device Name
172.29.112.73	B0:CA:68:5C:CF:58	Microsoft Windows 8.1
172.29.112.75	D0:33:11:D4:F9:DE	Microsoft Windows 8.1
172.29.112.80	AA:AA:AA:CC:CC:CC	Microsoft Windows 8.1
172.29.112.80	AC:E0:10:11:11:0F	Apple iPad
172.29.112.84	CC:44:63:97:8E:F5	Microsoft Windows 8.1
172.29.112.85	00:E0:4C:60:00:EF	Microsoft Windows 8.1
172.29.112.87	3C:18:A0:03:14:55	Microsoft Windows 8.1
172.29.112.88	00:25:90:25:12:94	Microsoft Windows 8.1
172.29.112.100	F4:4D:30:68:7C:61	Microsoft Windows 8.1
172.29.112.100	F4:4D:30:68:7C:61	Microsoft Windows 8.1
172.29.112.244	00:19:30:E6:D5:4F	Microsoft Windows 8.1
172.29.112.250	54:78:1A:8C:D4:CD	Cisco Networking Device
172.29.112.254	00:1B:8F:37:30:71	Cisco Networking Device

Pop-up windows for Apple iPad and Microsoft Windows 8.1 show detailed manufacturer information, including platform information, search engines, end of sales/support dates, and business status.

# 제품 특징점

## MacOS Agent



MacOS 로그인 팝업

## MacOS 노드 정보

OS	PT	액션명	플러그인명	설명
Microsoft Windows				
Apple OS X Mavericks				
Apple MacBook Pro				

## MacOS Agent 수집 정보

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

## Software 정보 수집

프로그램명	버전	제공 버전	MacOS 지원 버전	최근변경사시간	등록원시각
AirPort 유틸리티	6.3.2	apple	Apple OS X Yosemite	5/22/13, 5:05 AM	2018-04-04 09:38:54
App Store	1.3	apple	Apple OS X EI Capitan	5/14/13, 2:01 AM	2018-04-04 09:38:54
Apple OS X Mavericks	10.9.5	apple	Apple macOS Sierra		
Macintosh HD					
AppleScript 편집기	2.6.1	apple		4/25/13, 6:23 AM	2018-04-04 09:38:54
Automator	2.4	apple		4/20/13, 2:15 AM	2018-04-04 09:38:54
Bluetooth 파일 교환	4.2.7	apple		2/13/18, 12:18 PM	2018-04-04 09:38:54
Boot Camp 지원	5.1.2	apple		3/21/14, 8:19 AM	2018-04-04 09:38:54
Cocoa-AppleScript Applet	1.0	unknown		1/15/14, 2:17 PM	2018-04-04 09:38:54
ColorSync 유틸리티	4.9.0	apple		8/25/13, 2:57 PM	2018-04-04 09:38:54
Dashboard	1.8	apple		8/25/13, 10:38 AM	2018-04-04 09:38:54
Droplet with Settable Properties	1.0	unknown		1/15/14, 2:17 PM	2018-04-04 09:38:54
DVD 플레이어	5.7	apple		12/9/13, 2:44 PM	2018-04-04 09:38:54
FaceTime	3.0	apple		5/16/14, 8:44 AM	2018-04-04 09:38:54
Feedback Assistant	unknown			3/23/14, 4:56 AM	2018-04-04 09:38:54

# 제품 특징점

## Device Platform Auto Detection

- Agent 설치 없이도 플랫폼 자동 분류 엔진을 통해 네트워크 내의 장치에 대한 상세한 플랫폼정보를 제공합니다.

Genian NAC v5.0 관리 | 감사 | 정책

전체노드 / 플랫폼 현황

플랫폼	수량	비율
1 알수없음	254	20%
2 Genians Genian NAC	197	15%
3 Cisco Networking Device	81	6%
4 Microsoft		
5 Linux		
6 Microsoft		
7 MOIMST		
8 Microsoft		
9 Cisco C		
10 Ubuntu		
11 Apple M		
12 Apple D		
13 Apple IP		
14 Genians Genian		
15 Cisco Catalyst 2960 Switch	21	2%
16 Microsoft Windows 10 Pro	20	2%
17 Microsoft Windows 7 Professional	20	2%
18 Genians Genian GPI	19	1%
19 Moimstone IP255 VOIP Phone	18	1%
20 Stonehenge IP255-S 1.30.236	16	1%
21 Microsoft Windows 7 Professional x64	13	1%
22 Microsoft Windows 8.1 Home x64	11	1%
23 Microsoft Windows XP	10	1%

클라우드 기반 플랫폼 분석  
- 주 1회 플랫폼 정보 자동 update

전체노드 / 플랫폼 현황 / 지원종료

노드타입 전체 플랫폼 | 검색

\* 센서가 원격지에서 감지하거나 예측한 관리가능한 노드 플랫폼의 수를 의미합니다.

플랫폼	수량	비율
1 Microsoft Windows Server 2003	5	0%
2 Microsoft Windows Vista Business	4	0%
3 Cisco Catalyst 3550-24 Switch	2	0%
4 Aruba 200 Controller	1	0%
5 Citrix XenServer 6	1	0%
6 Citrix XenServer 7	1	0%

전체노드 / 플랫폼 현황 / 판매종료

노드타입 전체 플랫폼 | 검색

\* 센서가 원격지에서 감지하거나 예측한 관리가능한 노드 플랫폼의 수를 의미합니다.

플랫폼	수량	비율
1 Cisco Catalyst 2960 Switch	21	2%
2 Microsoft Windows 8.1 Pro	8	1%
3 Cisco Catalyst 3550-24 Switch	2	0%
4 Aruba 200 Controller	1	0%
5 Cisco Aironet 1600 AP	1	0%
6 Citrix XenServer 6	1	0%
7 Citrix XenServer 7	1	0%
8 Microsoft Windows 8.1 Professional x64	1	0%

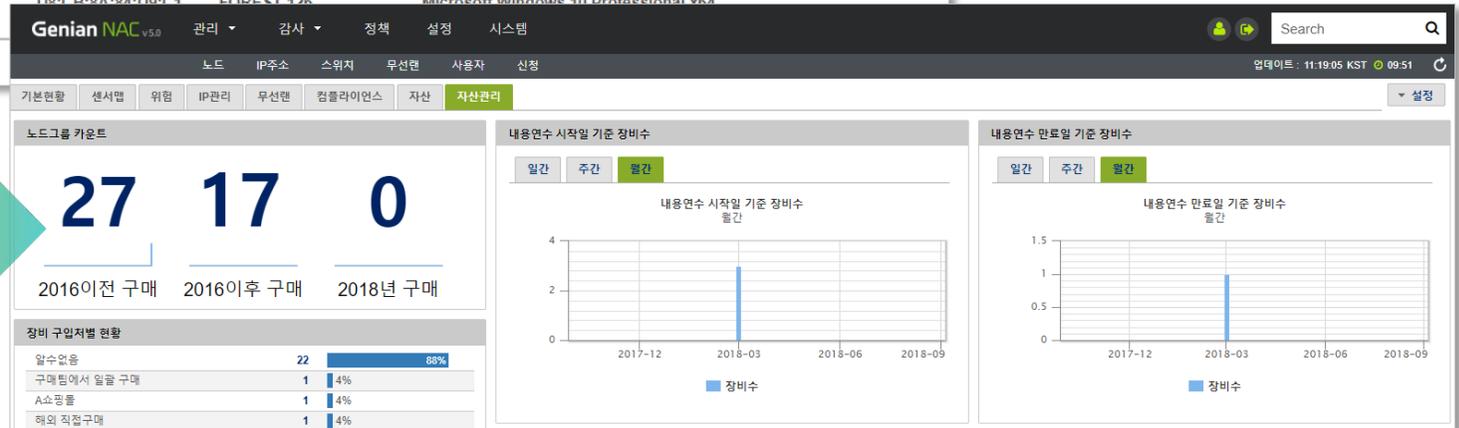
# 제품 특징점

## 장비 수명주기 관리

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								
<b>장비 수명주기 관리</b>									
제조일	2016-01-02	구입처	구매팀에서 일괄 구매						
내용연수 시작일	2016-01-05	내용연수	3	년	내용연수 만료일	2019-01-05			
내용연수 시작일과 내용연수를 설정하면 내용연수 만료일이 자동으로 입력됩니다.									
일련번호	123456789		구입가격	1,200,000					
책임자	김관리		책임부서	구매부					
메모									
장비내 노트	IP	MAC	호스트명	플랫폼					
	172.29.112.56	D8:CB:8A:84:D9:C1	FOREST_126	Microsoft Windows 10 Professional x64					

- 제조일, 내용 연한, 가격, 책임 부서 등 정보를 입력하여 그룹 설정 가능
- 대시보드에서 현황 관리 및 연한이 남은 장치에 대해서 사용자/관리자에 알림 기능을 제공

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



# 제품 특징점

## USB 장치 정보 자동 수집 및 조건 설정 그룹 생성

### 장치정보

- Bluetooth
  - Microsoft Bluetooth LE 열거자
  - Microsoft Bluetooth 열거자
  - Microsoft Bluetooth 프로토콜 지원 드라이버
  - MX Anywhere 2
- 네트워크 어댑터
  - Bluetooth Device (Personal Area Network)
  - Bluetooth Device (RFCOMM Protocol TDI)
- 마우스 및 기타 포인팅 장치
  - ELAN Input Device
  - HID 규격 마우스
- 카메라
  - NEC HD WebCam
- 키보드
  - HID 키보드 장치

### NAC 에 등록된 USB 정보

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

노드그룹: Webcam 사용 그룹

작업선택

NTAG SS	위험	동작	IP주소	MAC주소	정책	제어정책	호스트명(이름)	플랫폼
			172.29.112.56	D8:CB:8A:84:D9:C1		기본정책	FOREST-126	Microsoft Windows 10 Professional x64

Webcam 사용 그룹    1    AND    USB 장치 정보 / 장치명이 문자열을 포함하면 / WebCam

### 조건설정    USB 장치 기준 그룹 설정

항목: USB 장치 정보

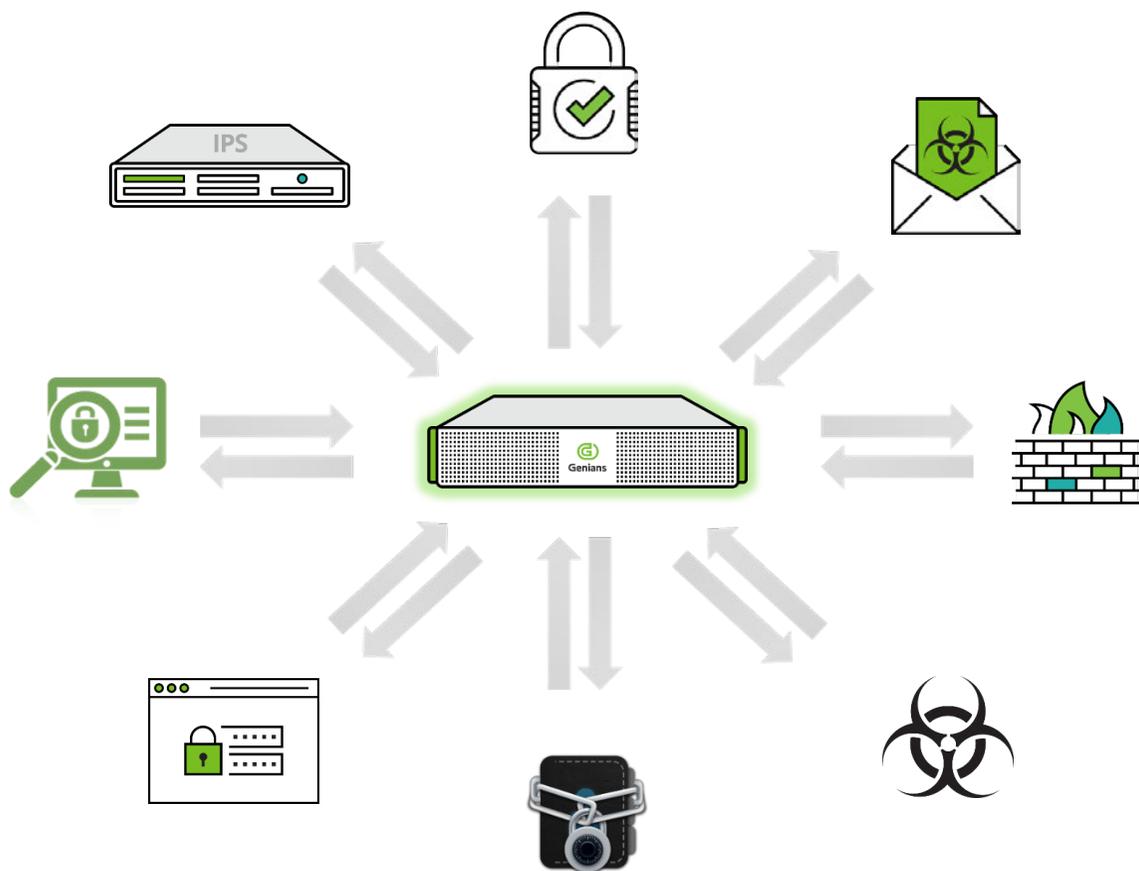
조건: 장치명이 문자열을 포함하면

설정: 특정 클래스가 존재하면

설정메모: USB장치명에 [설정내용] 문자열이 문자열을 포함하면

항목	조건	설정
USB 장치 정보	장치명이 문자열을 포함하면 ?	WebCam

## 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

# NAC 도입 후 네트워크 사용 절차

## 단계별 정책 준수 후 네트워크 허용 프로세스 구축

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/공유폴더 사용

보안 정책 준수 후 네트워크 사용

# 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. 보안 정책 미 준수 단말에 대한 네트워크 차단 및 필수 SW 설치 강제화
3. 인증을 통한 IP 실명제



별첨



# 주요 고객사

## 기업



## 금융



## 공공기관





Thank you!

문의 : 031)8084-9770

[sales@genians.com](mailto:sales@genians.com)