Genian NAC v5.0
제품소개서

지니언스

Genians

목 차

Part1, 개요

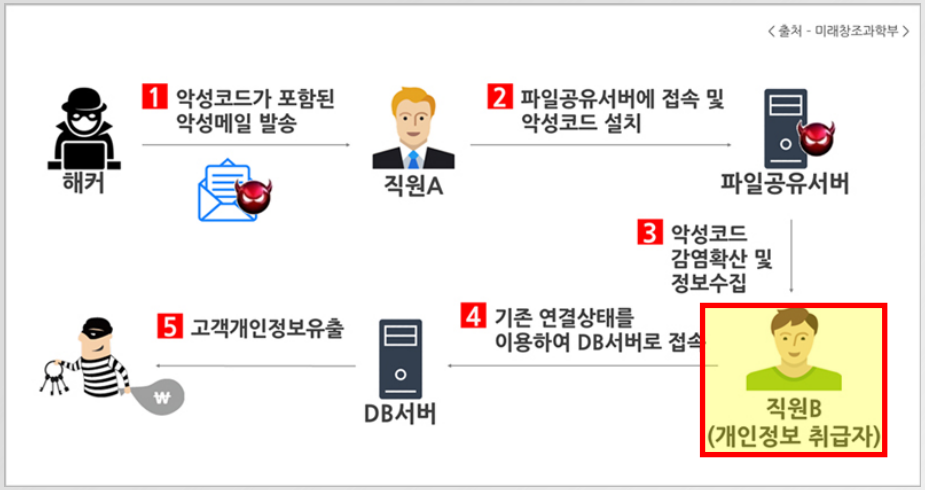
지속적인 내부 기술유출/보안 사고

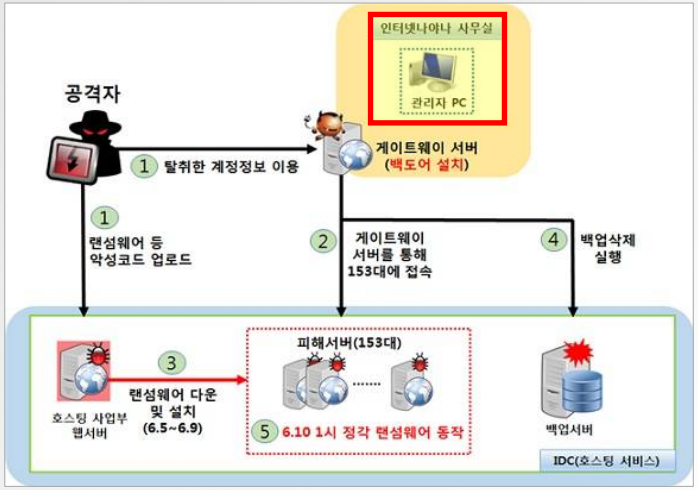
전통적인 방법의 기술유출과 지능적인 해킹

세 가지 방법의 전통적인 기술유출

1. 기업 내부 직원과 결탁하거나 인가된 제삼자 위탁업무를 빌미로 <u>기업에 접근해 저장 매체(USB Memory, Web Hard, CD 등)를 통해 불법적으로 기술을 빼가는 행위</u>
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

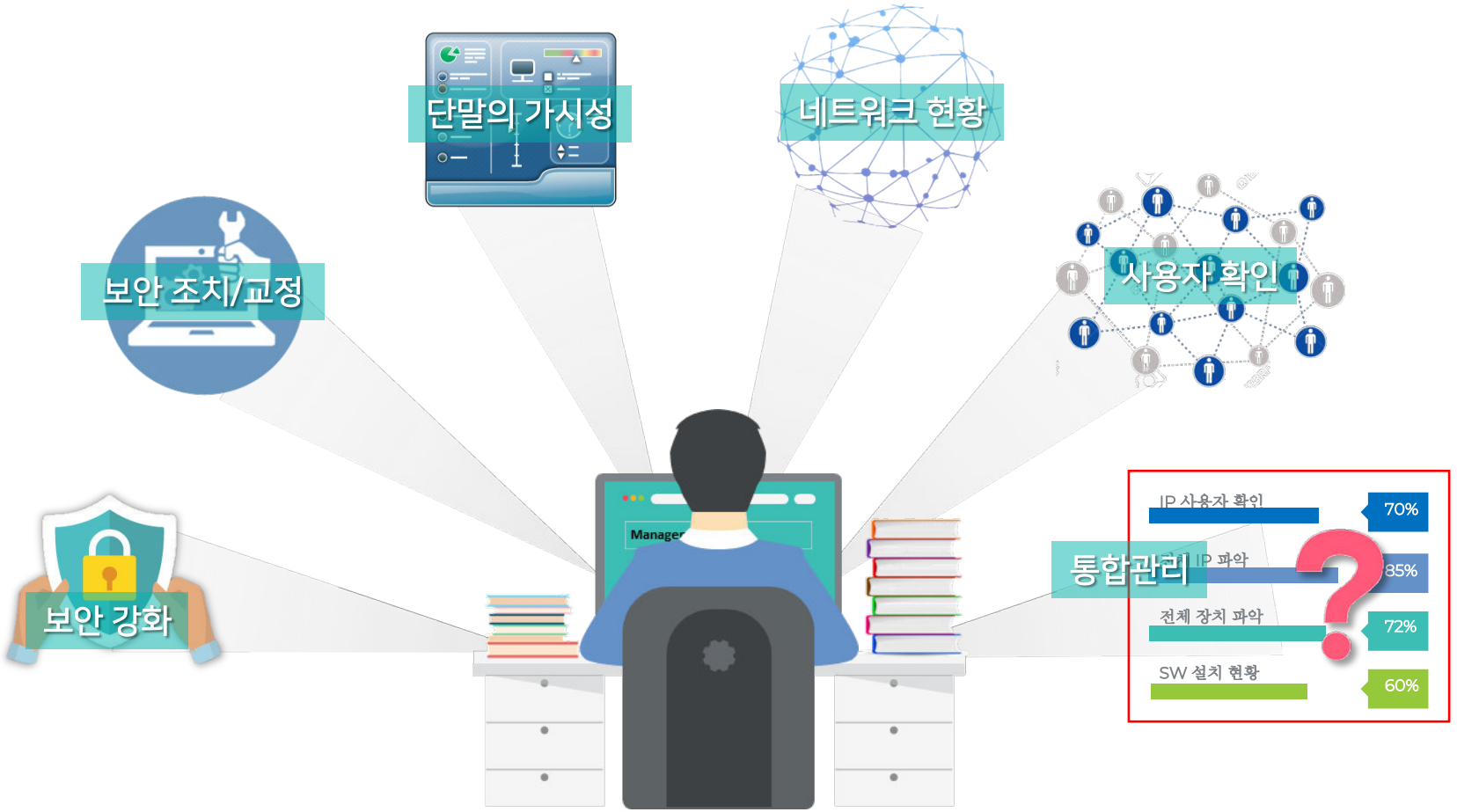
APT 공격의 주 목적은 정보 탈취 및 시스템 장악으로 시스템 접속 권한이 있는 <u>관리자 PC가 주요 표적</u>이 되고 있다





관리자의 고민

지속적인 보안 사고로 인한 관리자의 역할 증가

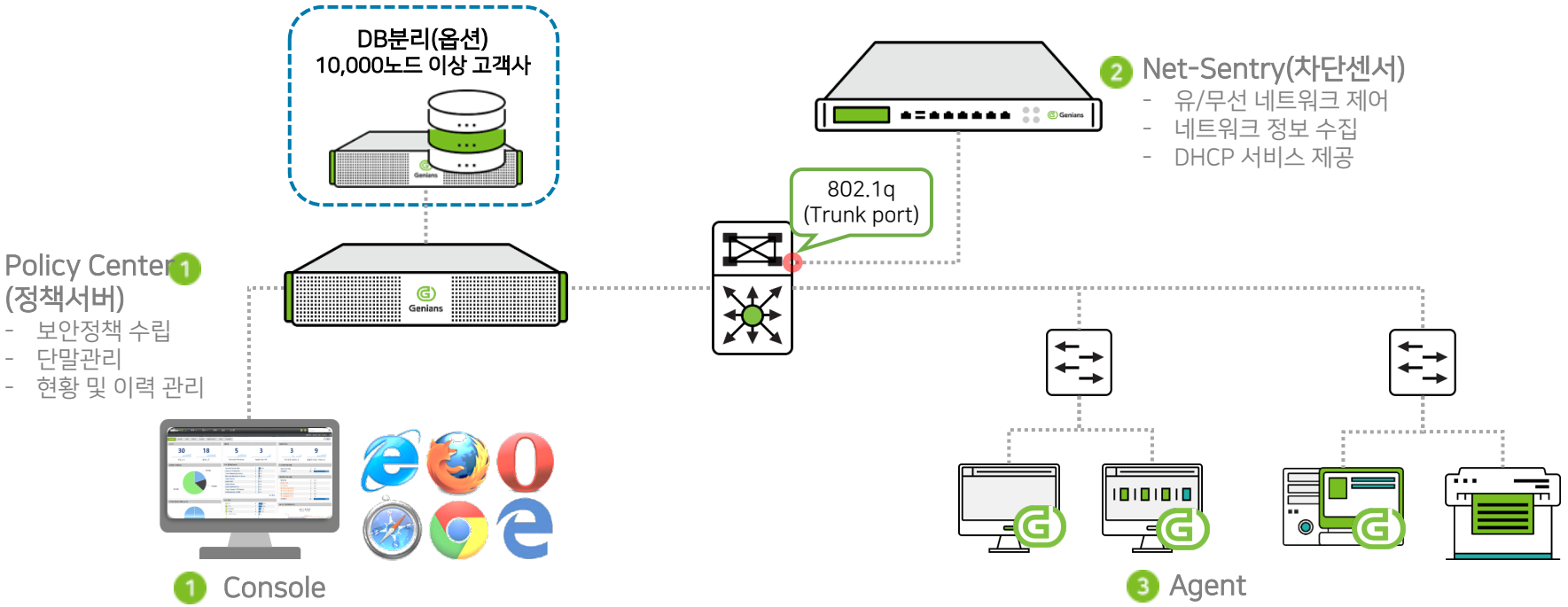


Part2,
Genian NAC
제품소개

관리 툴을 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

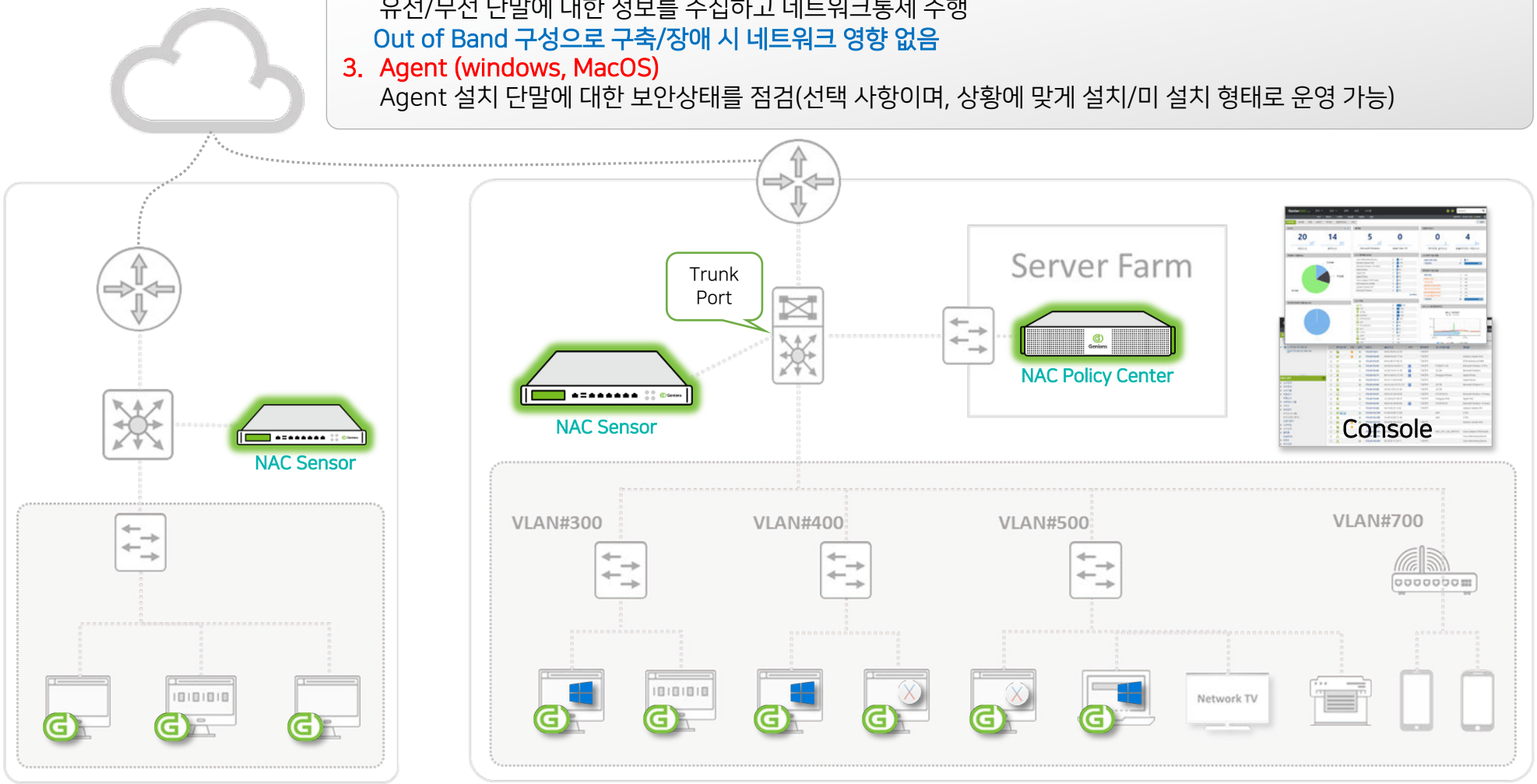
3 에이전트(Agent)

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)



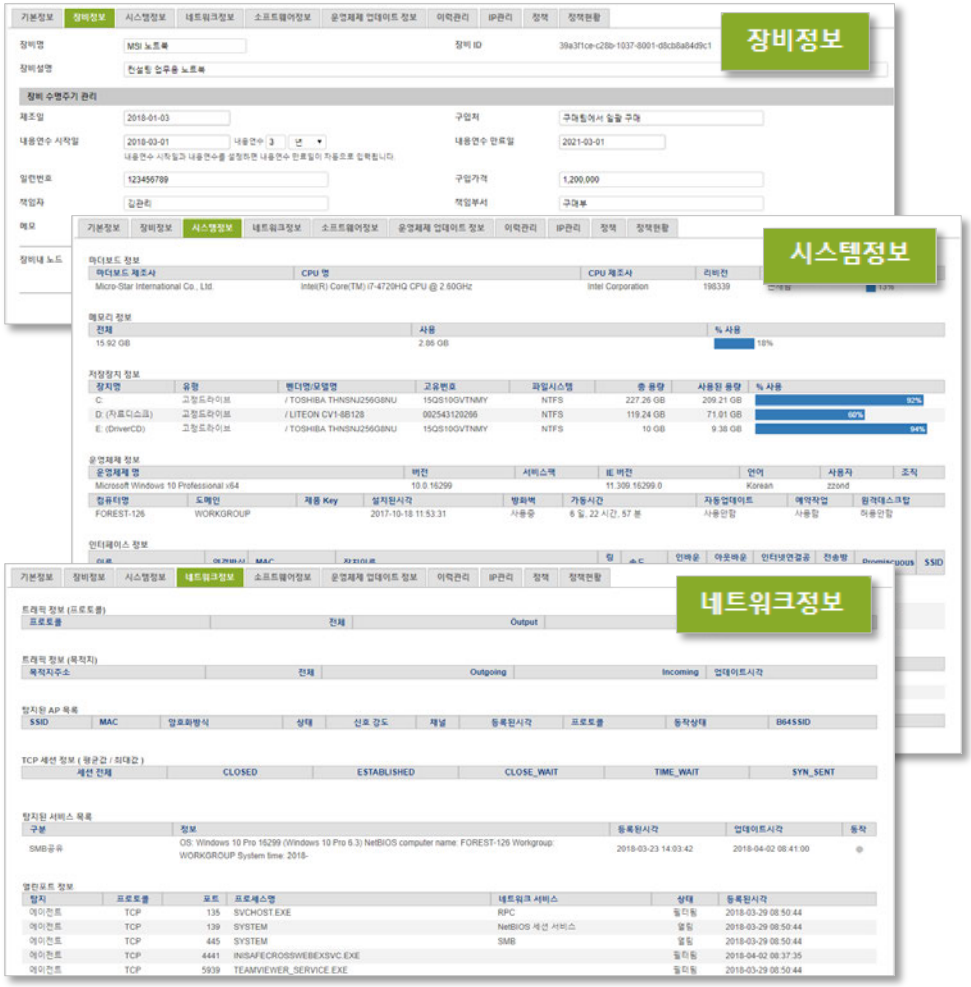
가시성 (1/3)

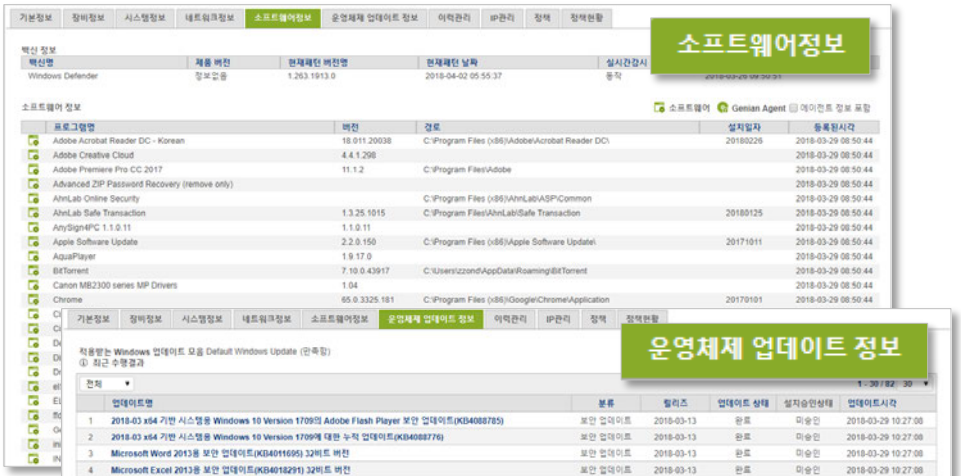
네트워크 내의 모든 단말기 정보 수집 및 분류, IP 실명 확인

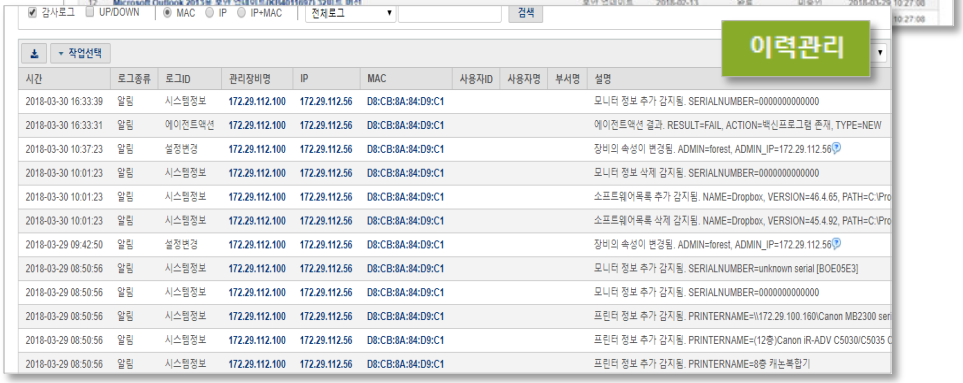
장치 구분	On/Off	가동률	인증 정보	인증 시간	연결된 스위치		IP/MAC		사용 위치	OS/장치 모델 상세 정보	서비스	최종연결시간	Hostname	NIC 제조사	동작 현황
NT AG SS	동작	가동률	인증사용자↓	최근 사용자인증	스위치	포트	IP주소	MAC주소	위치	플랫폼	서비스	마지막 동작시각	호스트명	NIC벤더	동작상태차트
		22%	황	2018-04-05 15:29:09			172.29.50.158	E4:70:B8:EE:5B:33	50.0 연구소IP대역	Microsoft Windows 10 Home x64			DESKTOP-9KISQBM	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.	
		15%	이	2018-04-05 09:55:04			172.29.50.237	7C:01:91:8B:7A:45	50.0 연구소IP대역	Apple Device		2018-04-05 09:57:46	yiho25-i6S	Apple, Inc.	
		25%	이	2018-04-04 15:59:32			172.29.50.238	54:26:96:CE:A0:07	50.0 연구소IP대역	Apple MacBook Pro		2018-04-05 14:56:55	MACBOOKPRO-A007	Apple, Inc.	
		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		2018-03-29 17:42:47	mars-iPhone	Apple, Inc.	
		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			mars-iPhone	Apple, Inc.	
		1%	이	2018-04-04 10:45:57			172.29.128.81	00:60:6E:B3:F6:39	128.0(이재열 팀장)	Microsoft Windows 10 Home		2018-04-04 11:02:40	이충우	DAVICOM SEMICONDUCTOR, INC.	

가시성 (2/3)

PC 내의 다양한 정보 제공

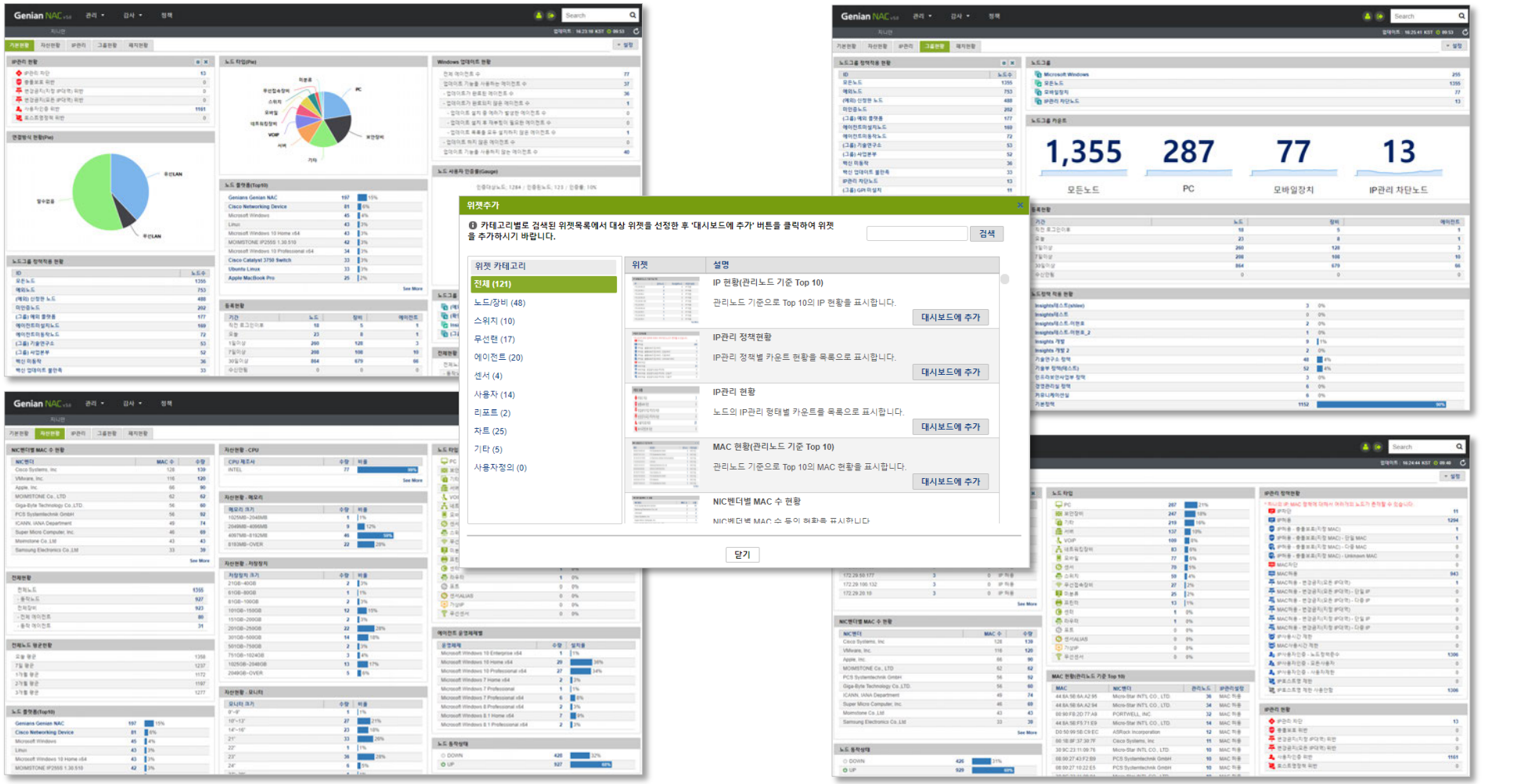






가시성 (3/3)

Dashboard 를 통한 다양한 통계, 상태 등의 현황 파악 용이



분류 (1/2)

다양한 분류 조건 제공(Dynamic Classification)

분류 조건

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%

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

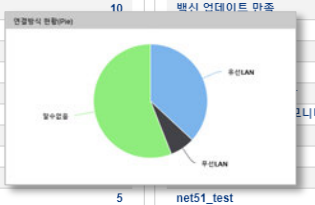
기간	노드	장비	에이전트
직전 로그인이후	22	2	1
오늘	51	11	2
1일이상	157	43	4
7일이상	328	197	10
30일이상	845	684	64
수신안됨	0	0	0

노드그룹 정책적용 현황

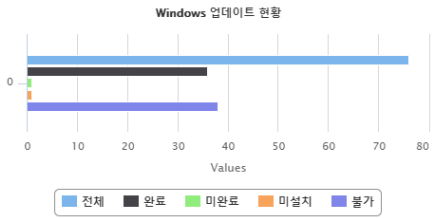
ID	노드수
모든노드	1381
예외노드	725
(예외) 신청한 노드	455
미인증노드	205
에이전트미설치노드	169
(그룹) 예외 플랫폼	162
에이전트미동작노드	57
(그룹) 기술연구소	49
(그룹) 사업본부	48
백신 미동작	40
백신 업데이트 불만족	37
IP관리 차단노드	10
Insights개발(이민상1)	
(그룹) GPI 미설치	
백신 실시간검사 미사용	
패치상태불만족노드	
(예외) 임시 예외노드	
Defender 모니터링 그룹	
PC	
(그룹) 경영관리실	
(그룹) 커뮤니케이션실	5
백신 미존재	4
(그룹) 신규사업TFT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



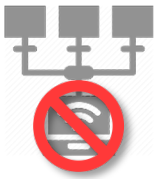
노드 태그

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

통제

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)

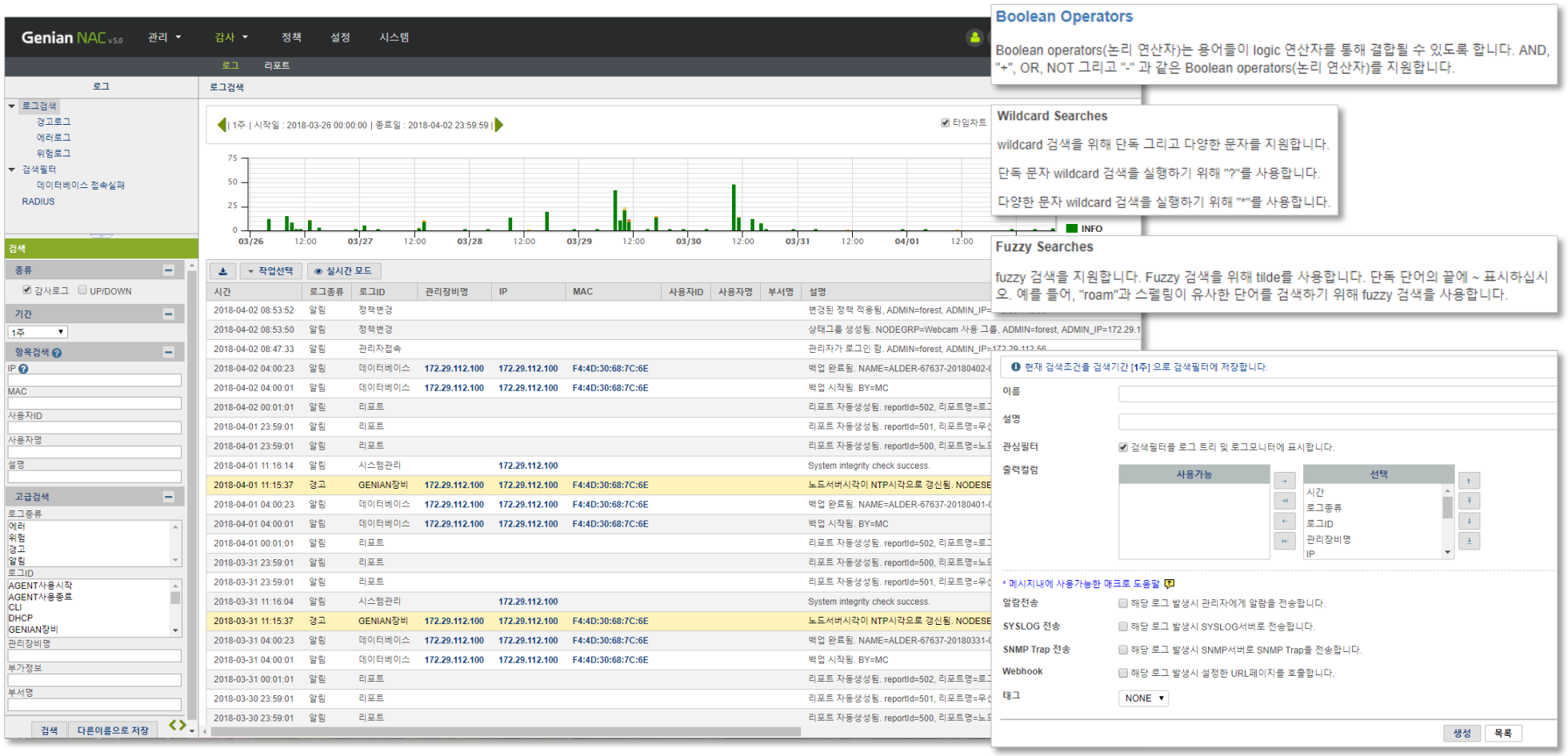
필수 SW 설치 유도
(백신, DRM, DLP 등
보안 솔루션 강제 설치)

불법 SW 삭제
(허용되지 않은 특정
SW 강제 삭제)

보안 설정 강제화
(패스워드 설정 유도,
화면보호기 강제 설정 등)

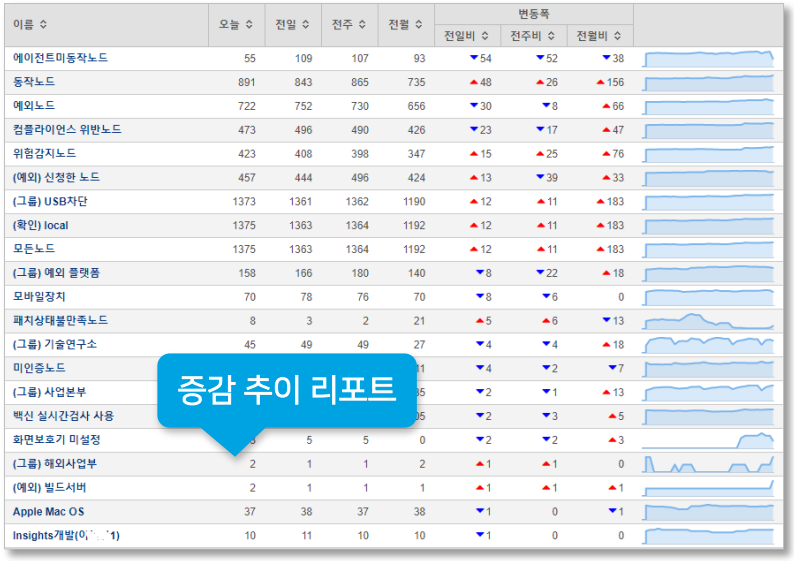
리포트 (1/2)

감사로그 필터링 & 로그 전송(SMS, E-mail, syslog, snmptrap)



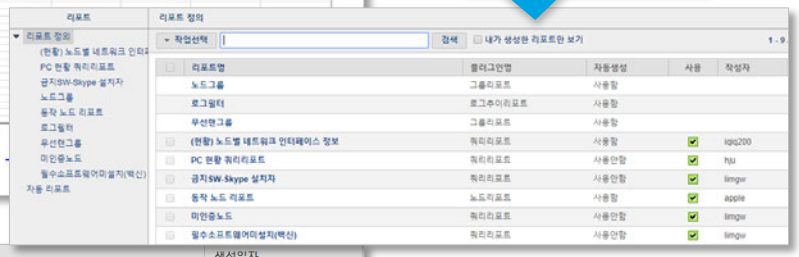
리포트 (2/2)

노드, 쿼리, 로그 Report 제공



증감 추이 리포트

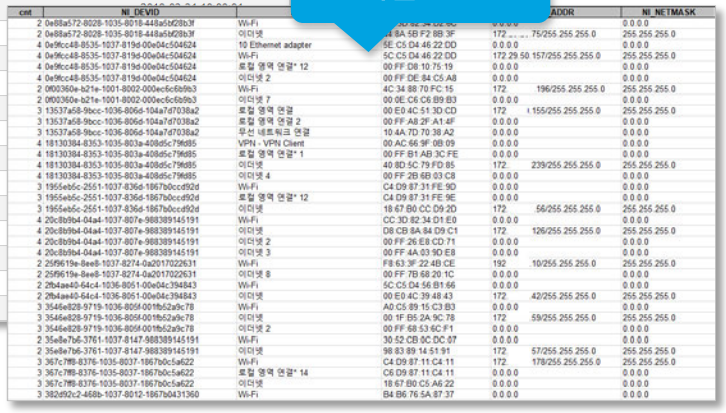
그래프 리포트



리포트 현황

스케줄 기능

쿼리 리포트
(관리자 지정)



엑셀 변환

Genian NAC 기능 요약

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, Wi-Fi, 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, 공유폴더 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

Windows

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

제품 특장점

단말 플랫폼 인텔리전스(DPI)

Genians

SOLUTIONS GENIAN NAC RESOURCES COMPANY TRIAL & 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.

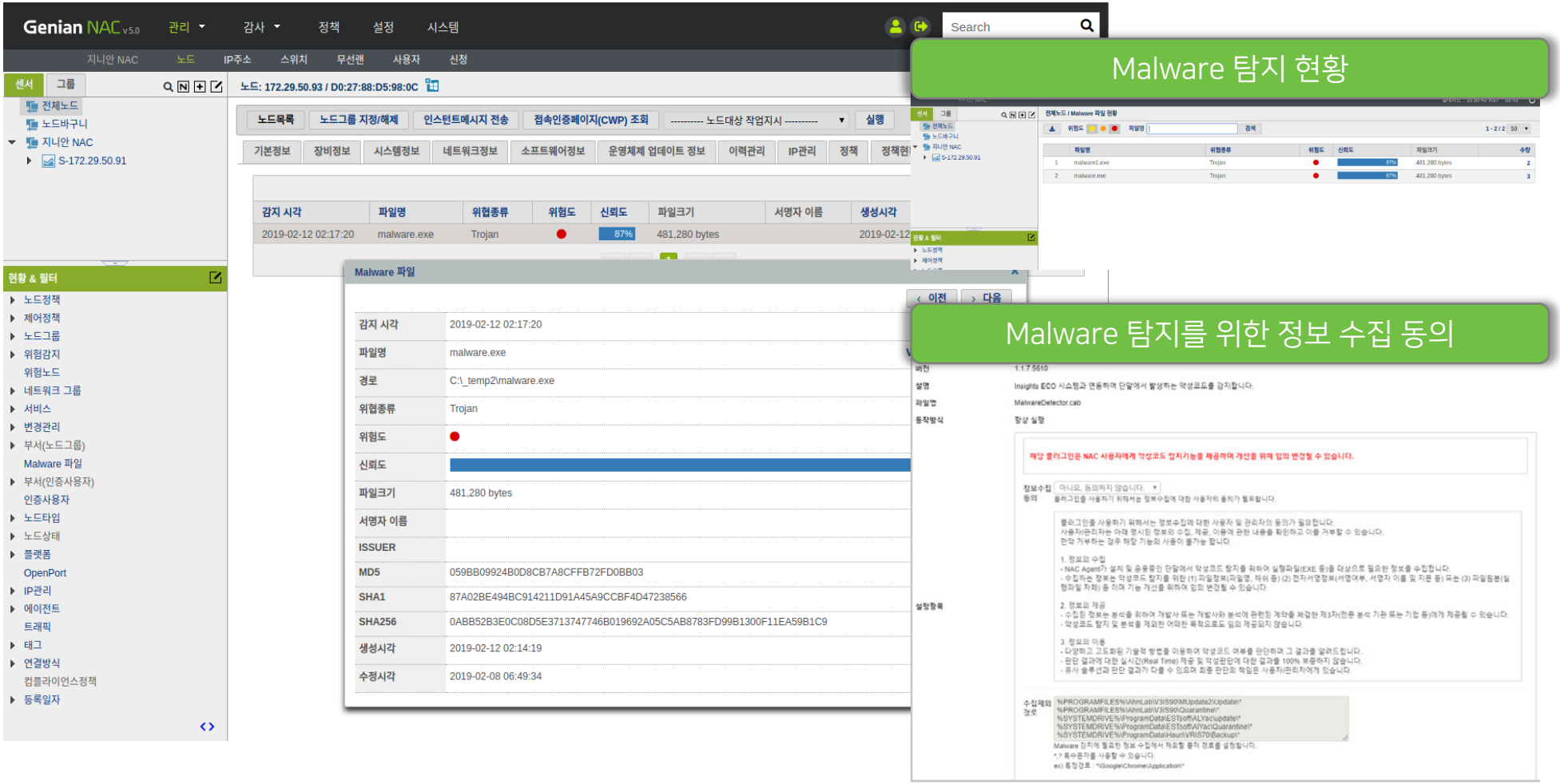
단말 및 제조사 취약점 정보
(CVE No/Severity/Description)

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

제품 특장점

단말에서 발생하는 악성코드를 탐지



제품 특장점

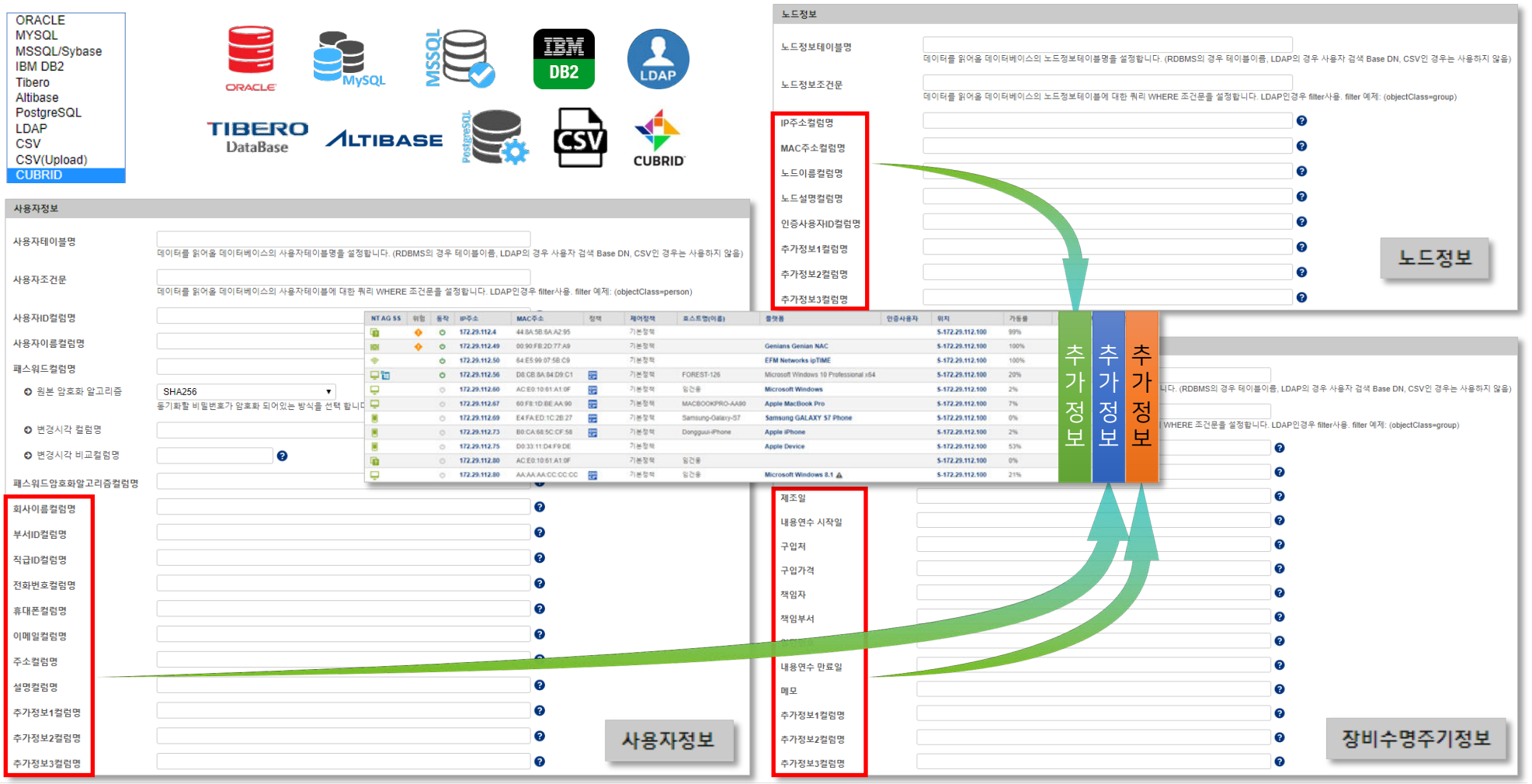
SAML (G-Suite 인증)

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.

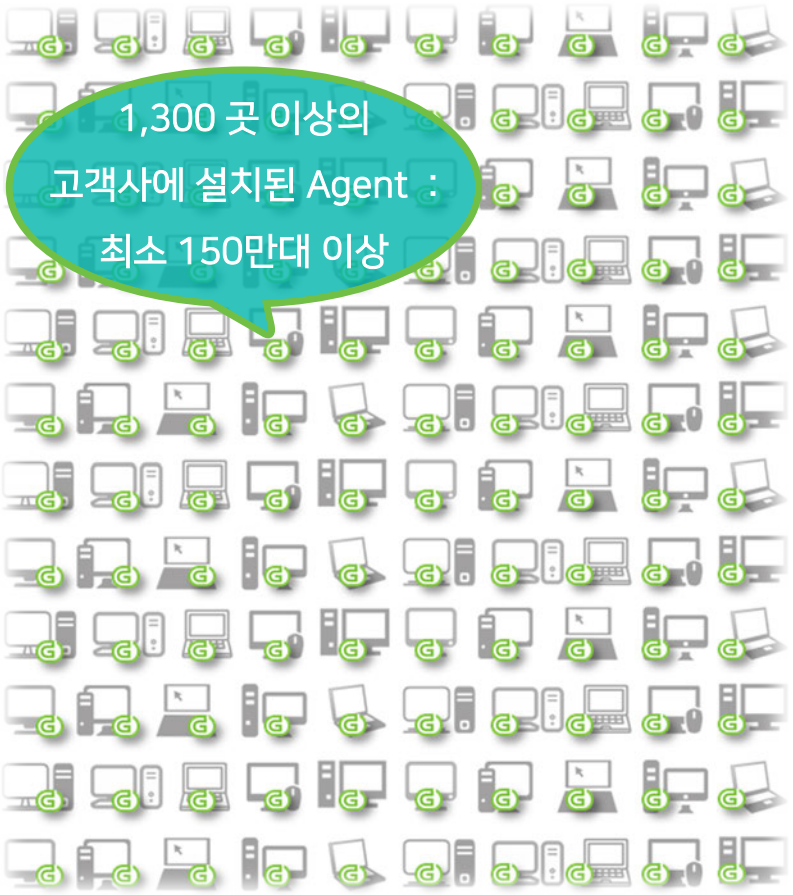
제품 특장점

다양한 DB와의 연동을 통해 NAC 에 특정 정보 자동 등록/관리



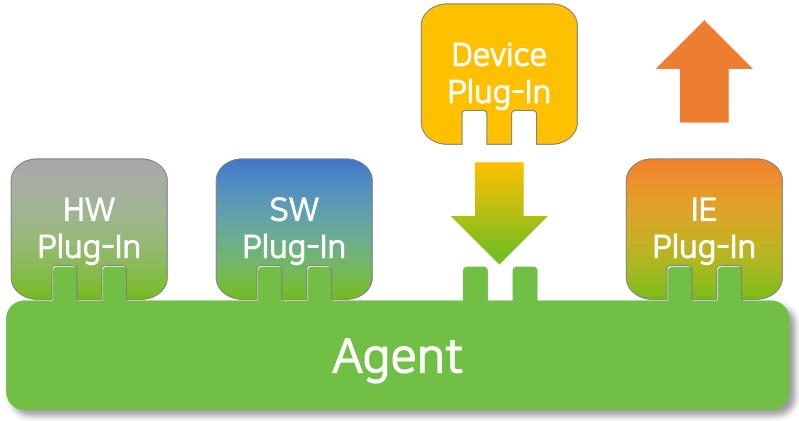
제품 특장점

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)

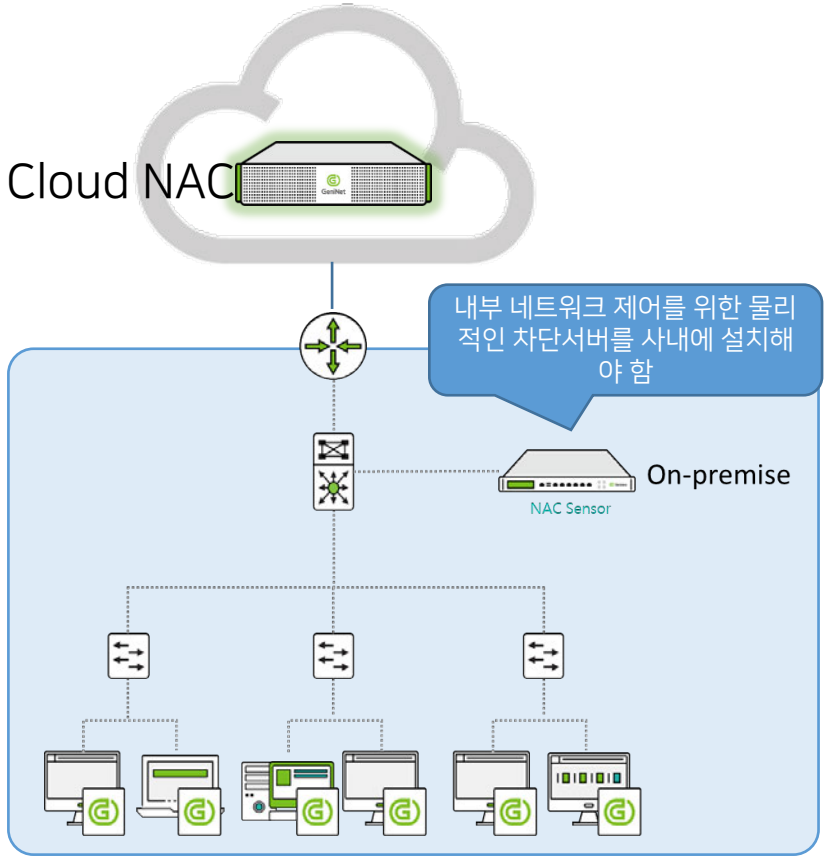
OS ↓	PT	액션명	플러그인명	설명
		사용자 알림메시지	사용자 알림메시지	사용자에게 알림메시지를 표시합니다.
		프로그램 제거	프로그램 제거	제어판의 프로그램 제거에 등록된 프로그램중 제거 가능한 특정 프로그램을 제거합니다.
		DNS 제어	DNS 제어	DNS 관련 로컬설정을 제어합니다.
		유선랜 인증 프로파일 설정	유선랜 인증 프로파일 설정	유선인터페이스의 802.1x 인증 프로파일 설정을 강제화 한다.
		네트워크 트래픽 제어	네트워크 트래픽 제어	주기적으로 네트워크 사용량을 수집하여 설정된 수치 이상일 경우 네트워크 인터페이스를 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.



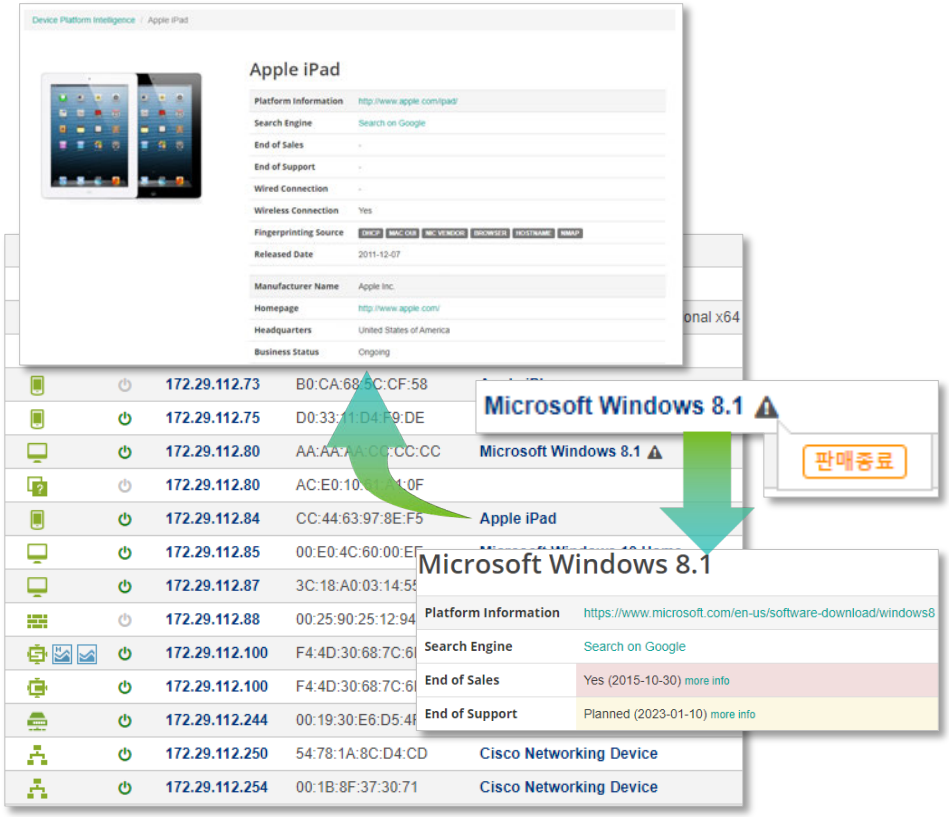
제품 특장점

Cloud NAC / Device Platform Intelligence

- 클라우드 서비스를 이용한 정책서버 구성(AWS)

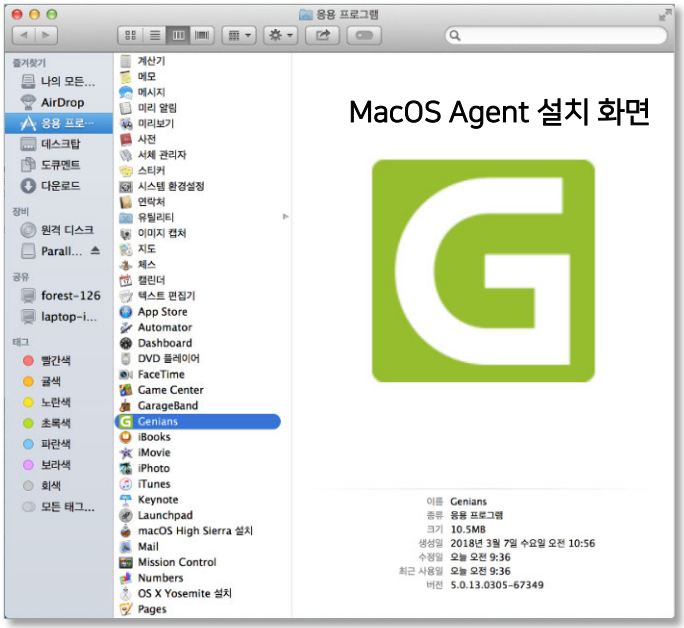


- 장치에 대한 제조사 지원 현황 제공 (홈페이지, 제조사, 판매상태 등)

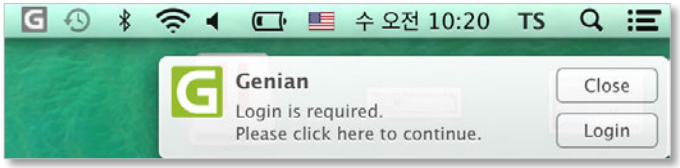


제품 특장점

MacOS Agent



MacOS Agent 설치 화면



MacOS 로그인 팝업

MacOS 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

MacOS Agent 수집 정보

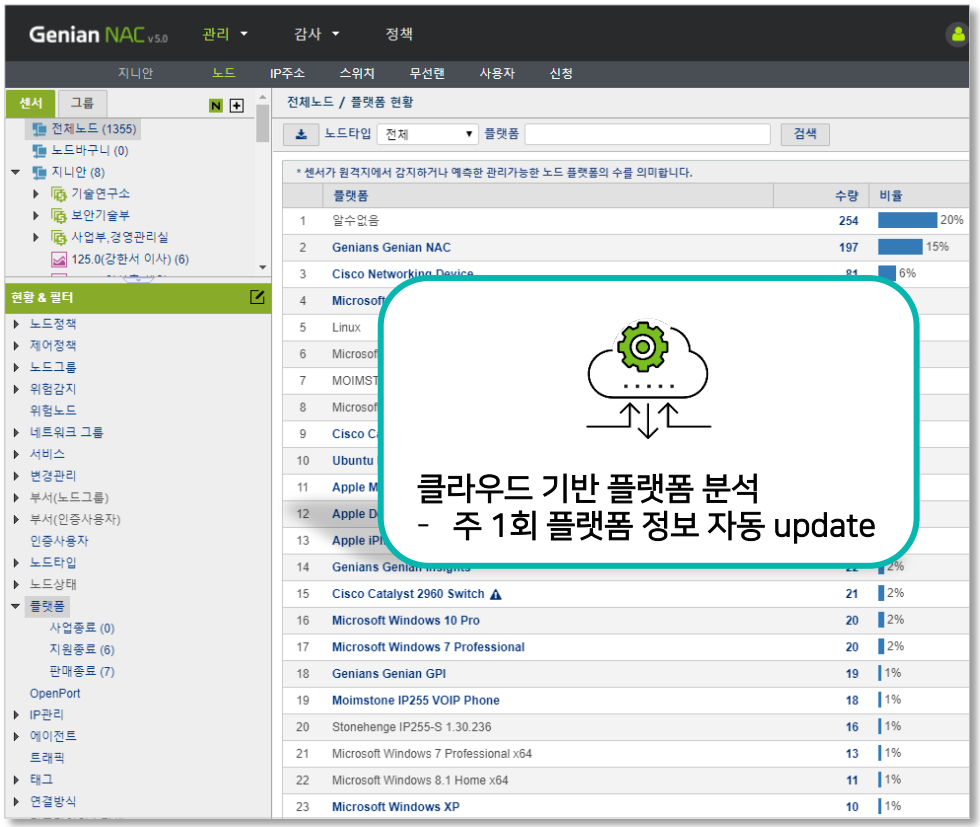
OS ↑	PT	액션명	플러그인명	설명
		운영체제정보 수집	운영체제정보 수집	macOS 운영체제 정보 및 사용자 정보를 수집하여 노드정보에 표시합니다.
		하드웨어정보 수집	하드웨어정보 수집	마더보드 정보, 메모리정보, 저장장치 정보를 수집하여 노드정보에 표시합니다.
		소프트웨어정보 수집	소프트웨어정보 수집	설치된 소프트웨어정보를 수집하여 노드정보의 [소프트웨어정보]-[소프트웨어목록]에 표시합니다.
		네트워크정보 수집	네트워크정보 수집	네트워크 인터페이스 정보를 수집하여 노드정보에 표시합니다.
		백신정보 수집	백신정보 수집	PC에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

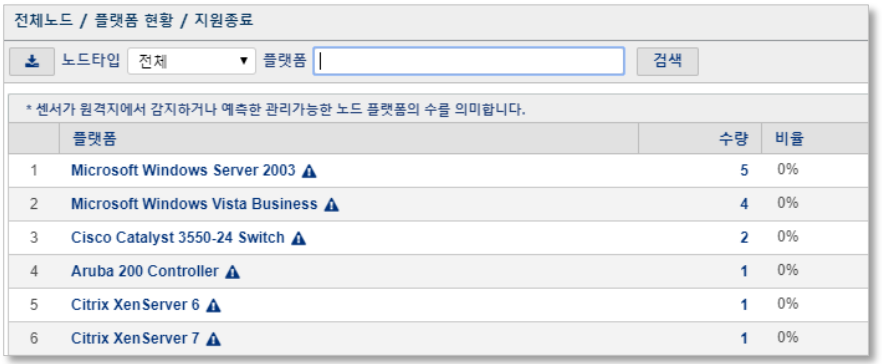
Software 정보 수집

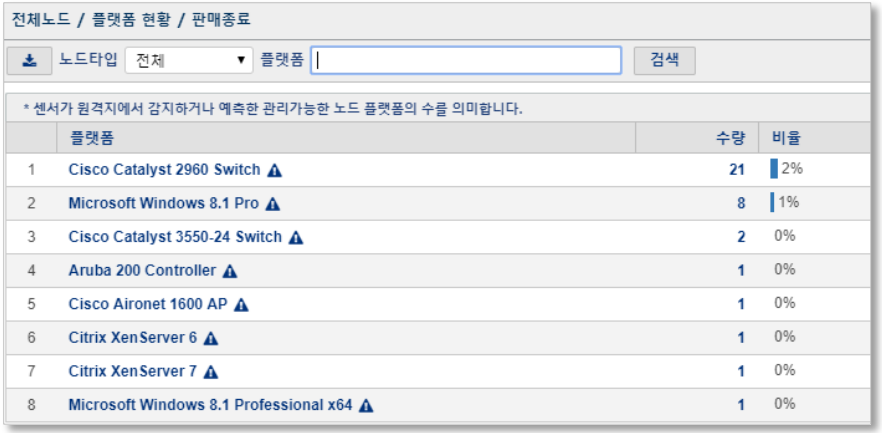
제품 특장점

Device Platform Auto Detection

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

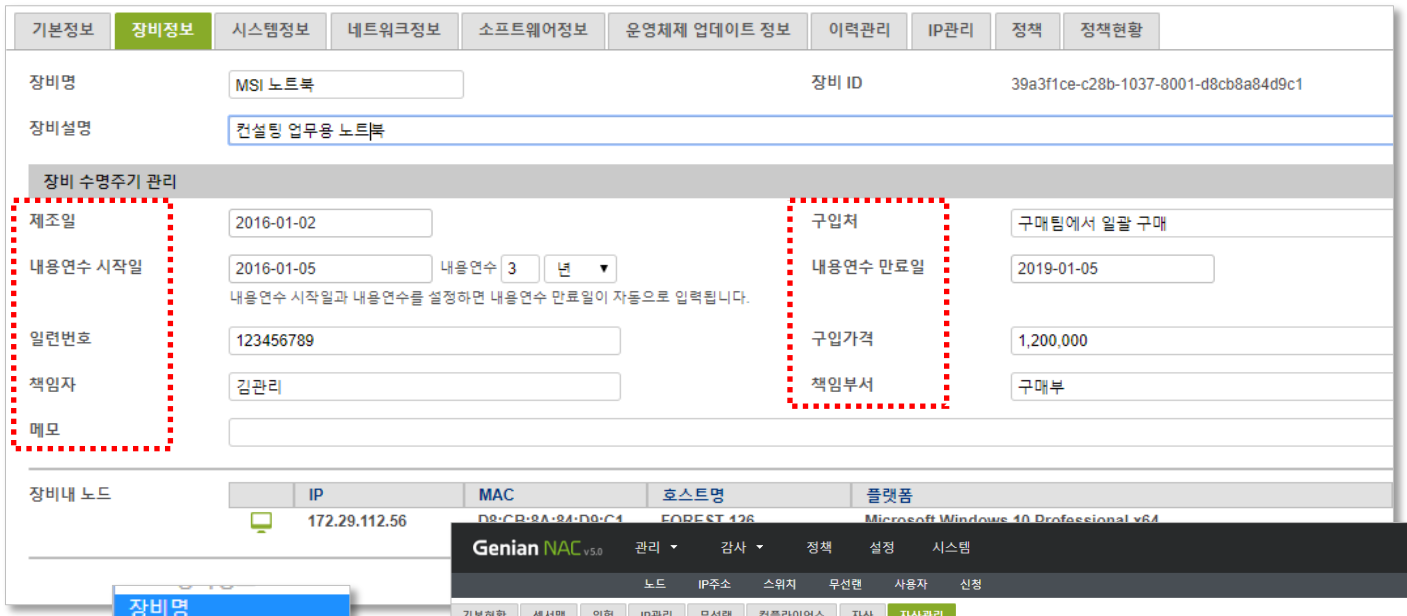


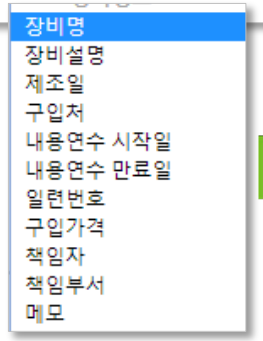


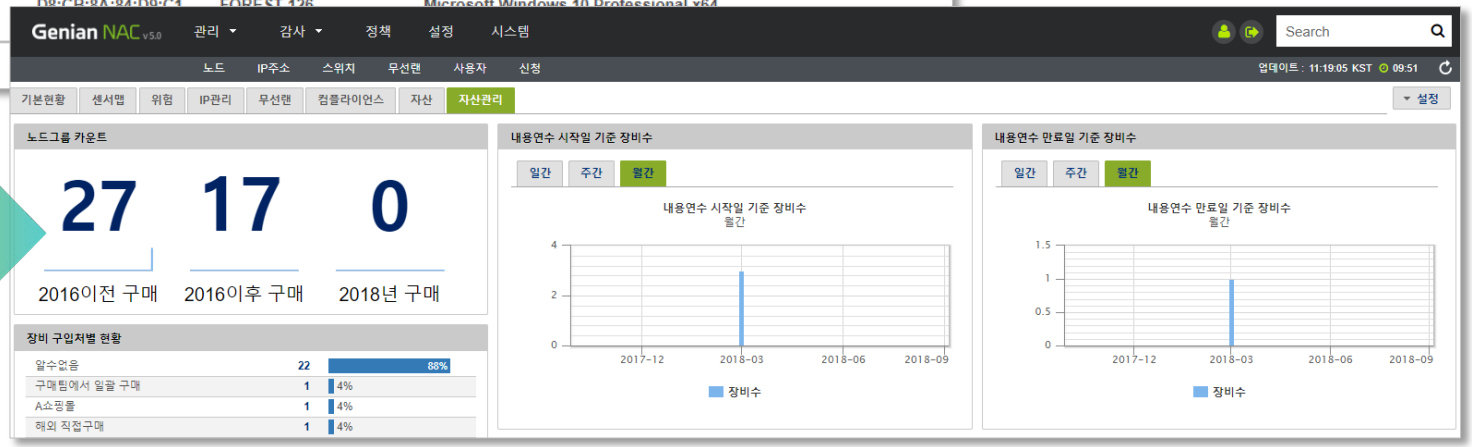


제품 특장점

장비 수명주기 관리





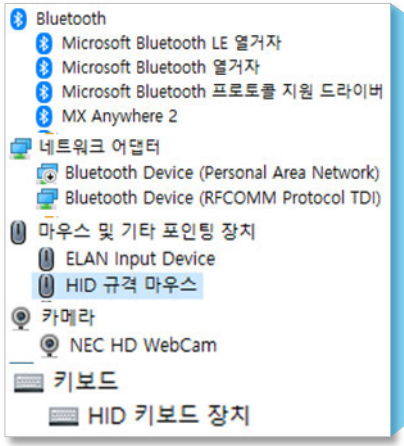


- 제조일, 내용 연한, 가격, 책임 부서 등 정보를 입력하여 그룹 설정 가능
- 대시보드에서 현황 관리 및 연한이 넘은 장치에 대해서 사용자/관리자에 알림 기능을 제공

제품 특장점

USB 장치 정보 자동 수집 및 조건 설정 그룹 생성

장치정보

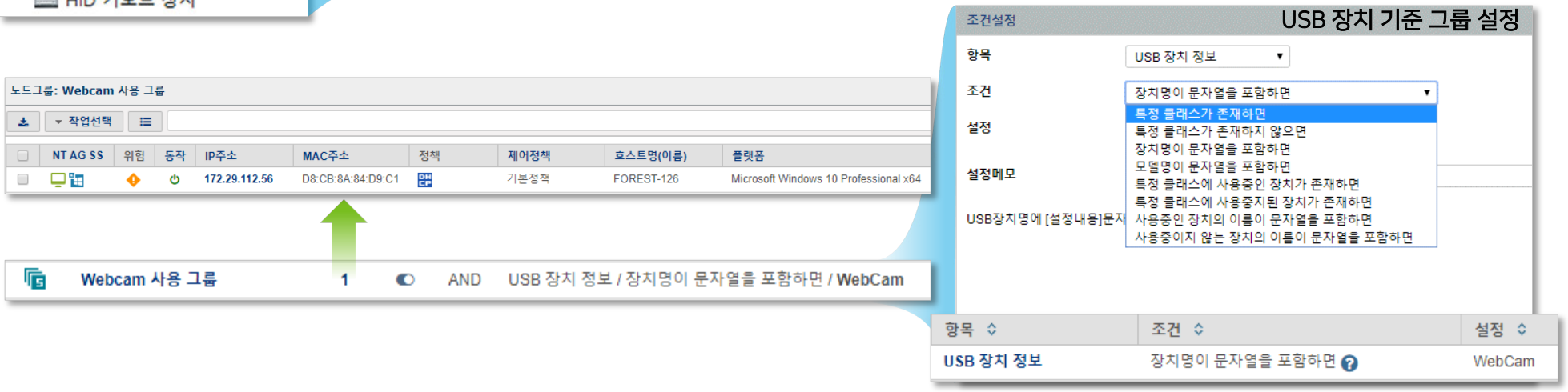


NAC 에 등록된 USB 정보

USB 정보

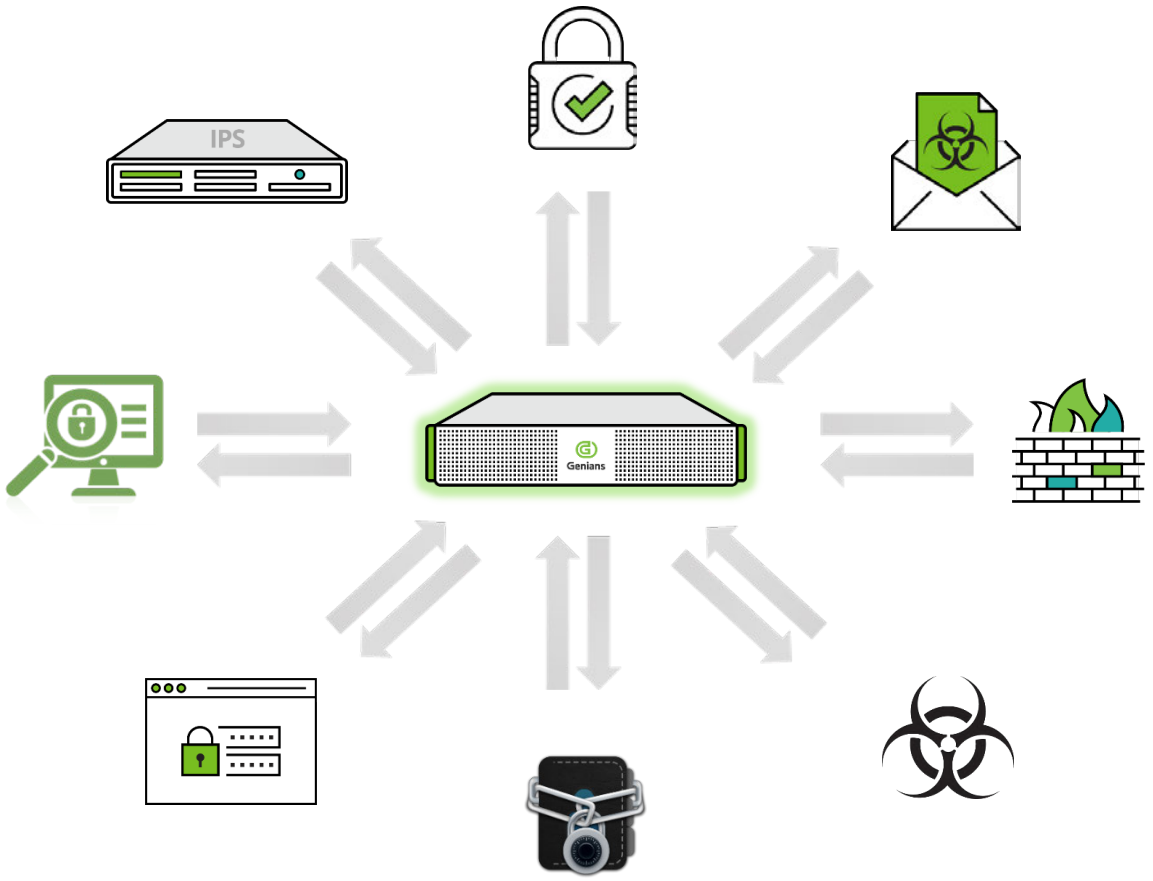
클래스명	장치명	제조사	모델명	시리얼	상태
Bluetooth	MX Anywhere 2				사용
Bluetooth	Microsoft Bluetooth 열거자				사용
Bluetooth	Microsoft Bluetooth 프로토콜 지원 드라이버				사용
네트워크 어댑터	Bluetooth Device (Personal Area Network)				사용중지
네트워크 어댑터	Bluetooth Device (RFCOMM Protocol TDI)				사용
키보드	HID 키보드 장치	Logitech	USB Receiver		사용
마우스 및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

USB 장치 기준 그룹 설정



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

NAC 도입 후 네트워크 사용 절차

단계별 정책 준수 후 네트워크 허용 프로세스 구축

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