




내부 인프라 통합관리 및 보안강화를 위한

Genian NAC Suite



목 차

-
- 네트워크접근제어(NAC)의 필요성
 - Genian NAC suite Suite 소개
 - 지니네트웍스 회사소개
-

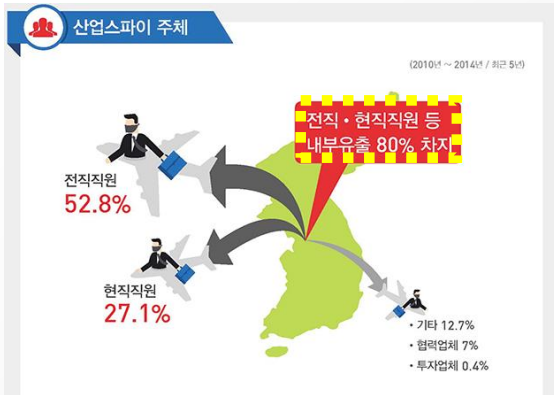


네트워크 접근 제어
(NAC)의 필요성

내부정보 유출사고

내부 정보 유출 방지 및 사용자 네트워크 제어를 위한 NAC

※ 출처: 산업기밀보호센터



✓ 산업 스파이 정보유출에 대한 이슈 사항

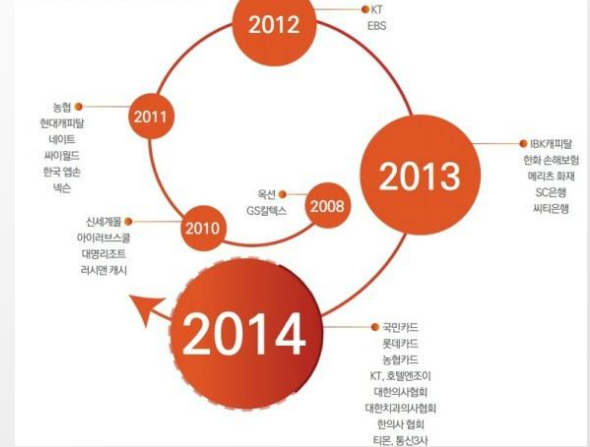
- 전직 직원 내부 접근
- 현직 사용자 중요 정보 접근
- 외부 저장 장치에 대한 통제
- 스마트폰 등의 모바일 환경 통제
- 보안시스템 우회



✓ 개인정보 유출 사고에 대한 이슈 사항

- 전직/현직 직원 중요 정보 접근
- 외주 직원 중요 정보 접근
- 내부/외부 직원 구분
- 외부 저장 장치에 대한 통제
- 보안시스템 우회

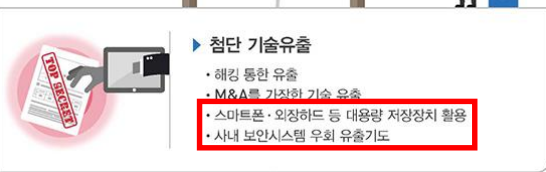
주요 개인정보유출 사고 일지



고객 정보 유출된 금융회사

시기	회사	유출건수	유출경로
2011년3~5월	한화손해보험	15만여건	외부 해킹
2011년4월	현대캐피탈	175만여건	외부 해킹
2011년7월	하나SK카드	9만여건	내부 직원
2010년1월~2011년8월	삼성카드	80만여건	내부 직원
2011년12월~2012년2월	한국SC은행	10만3000여건	외주 직원
2011년12월~2012년3월	IBK캐피탈	5800여건	내부 직원
2013년2~5월	메리츠화재	16만여건	내부 직원
2013년4월	한국씨티은행	3만4000여건	내부 직원
2012년10월~2013년12월	KB국민카드, 롯데카드, 농협카드	1억400만여건	외주 직원

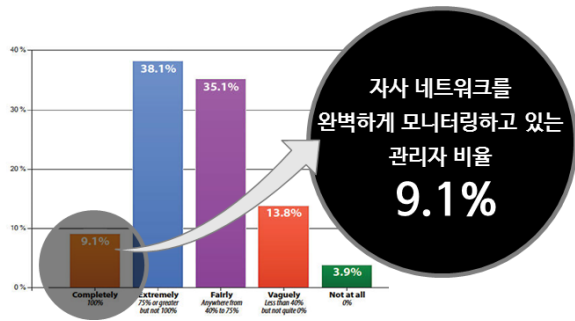
산업스파이 범죄 수법 첨단화·지능화·고도화



Visibility

IT환경의 변화로 내부 네트워크에 연결된 단말 및 장치 현황, 단말기의 상태, 사용자 접속 현황에 대한 **가시성**과 상태에 따른 **통제** 필요

네트워크 가시성



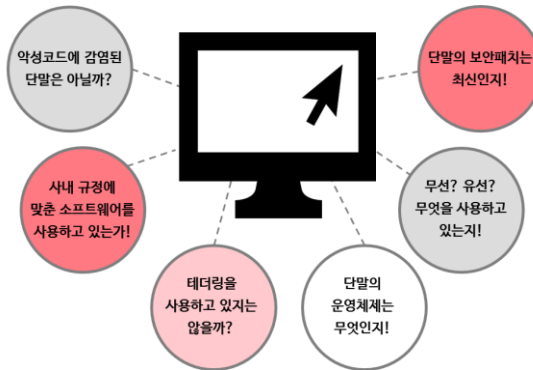
<출처 : SANS BYOD Security Survey(2012)>

네트워크 단말의 수량 및 다양성 증가

사용자 가시성



단말의 가시성



관리 노드 (1 - 1 / 1)							
IP	R	IP	IP주소	MAC주소	정책	네트워크정책	설명
			192.168.1.237	00:24:07:E9:34:14		(RBAC)실업체	외부 컨설팅 인원

도메인	종류	인증사용자	최근동작	스위치.포트
WORKGROUP	Microsoft Windows 7 Ultimate x64	이상협	2012-05-18 13:53:23	Switch248.geninetwoks.com G11/0/10

보안규정의 시행 강화

업종별 내부 보안 규정시행 - 기업(관)의 내부 보안에 대한 적절한 보호조치 요구

-공통항목-

사용자 권한에 따른 네트워크 접근통제 단말기 보안 무결성 등

(안전행정부)개인정보보호법

(안전행정부)정보통신 보안업무규정

(방송통신위원회)정보보호 관리지침

(금융위원회) 금융전산 망분리 가이드라인

(금융위원회) 금융전산 보안 강화 종합대책

(방송통신위원회)모바일 오피스 정보보호수칙

(보건복지부)의료기관 개인정보보호 가이드라인

(금융감독원)금융권 스마트워크 정보보호 가이드라인

(방송통신위원회)개인정보의 기술적, 관리적 보호조치 기준

(금융위원회/금융감독원)금융회사 정보기술(IT)부문 보호업무 모범규준

(안전행정부) 주요정보통신기반시설 기술적 취약 분석 평가방법 상세 가이드

...

(방송통신위원회)정보보호 관리지침

□ 접근통제 장치 확대 및 시스템 접속시간 제한 (안 제4조제9항 및 제10항)

- 현재 개인정보취급자의 "컴퓨터"에만 접근통제 조치를 하고 있으나, 태블릿PC 등으로 업무환경이 변화됨에 따라 "모바일 기기"를 추가함
- 개인정보처리시스템에 대한 접속이 필요한 시간에 한하여 유지되도록 "최대 접속시간 조치" 등을 취하도록 함

□ 개인정보 저장장치 확대 (안 제6조제4항)

- 현재 개인정보를 저장할 때 암호화해야 하는 장치를 "컴퓨터"에 한정하고 있으나, "모바일 기기 및 보조저장매체"를 추가함

□ 물리적 접근 방지 근거 마련 (안 제6조 신설)

- 보조저장매체 등을 통한 개인정보 유출을 막기 위해 전산실, 자료보관실 등에 대한 출입통제, 보조저장매체의 반출입 통제 근거를 신설함

전자금융거래법 (전자금융거래법 및 전자금융감독규정)	비교 (개인정보보호법 기준)
<ul style="list-style-type: none"> • 정보보호최고책임자는 전자금융거래 안전성 확보 등 계획 수립(법§21의23) • 금융기관 또는 전자금융업자는 정보기술부문 계획을 매년 수립·운영(§19) • 전산자료, 시스템, 해킹 및 악성코드 방지 등 분야별 보호대책 수립(§8, §13~§18) 	<ul style="list-style-type: none"> • 주요 내용 사실상 일치 (단, 내부관리계획 수정이력 관리는 다소 상이)
<ul style="list-style-type: none"> • 업무담당자 이외의 자가 단말기를 무단 조작 못하도록 단말기별 취급자 및 비밀번호 지정 사용자계정과 비밀번호 개인별 부여, 전산자료는 사용자 업무별로 접근권한 통제(§12~§13) 	<ul style="list-style-type: none"> • 주요 내용 사실상 일치 (단, 사용자 계정 공동사용을 예외적으로 허용하는 것은 다소 상이)
<ul style="list-style-type: none"> • 인출·회계 등 "인사조치"가 지체없이 해당 사용자 계정삭제·계정사용 중지·공동사용계정 변경 등 접근통제(§13조) • 사용자 계정 공동사용이 불가피한 경우 개인별 사용내역 관리 	
<ul style="list-style-type: none"> • 비밀번호 작성규칙 및 입력오류시 조치 방법 명시(§32) 	<ul style="list-style-type: none"> • 주요 내용 사실상 일치

(※ 개인정보보호법 제29조, 시행령 제30조, 안전성 확보조치 기준 고시)

연관성 확보 조치	내용
관리적 조치	<ul style="list-style-type: none"> ▶ 내부관리계획의 수립/시행
기술적 조치	<ul style="list-style-type: none"> ▶ 접근 권한의 관리 ▶ 비밀번호 관리 ▶ 접근통제 시스템 설치 및 운영 ▶ 개인정보 암호화 ▶ 접속기록의 보관 및 유출조 방지 ▶ 보안 프로그램(백신, 방화벽 등)의 설치 및 운영
물리적 조치	<ul style="list-style-type: none"> ▶ 개인정보의 안전한 보관을 위한 보관시설 ▶ 접근방지 설치

의료기관 개인정보보호 가이드라인 중

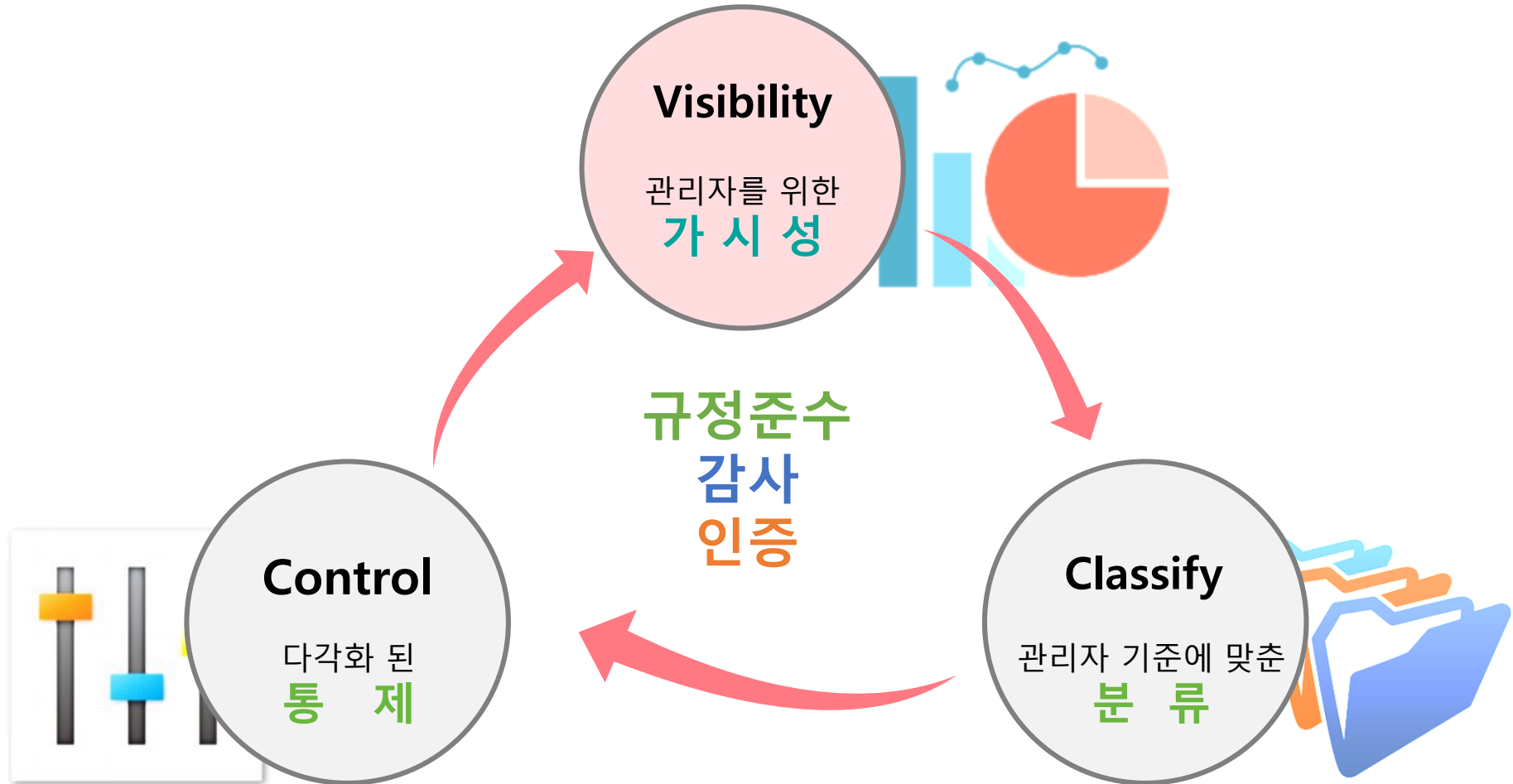


Genian NAC suite Suite

소개

Genian NAC suite

가시성 확보를 통한 분류, 다양한 네트워크 통제 기능



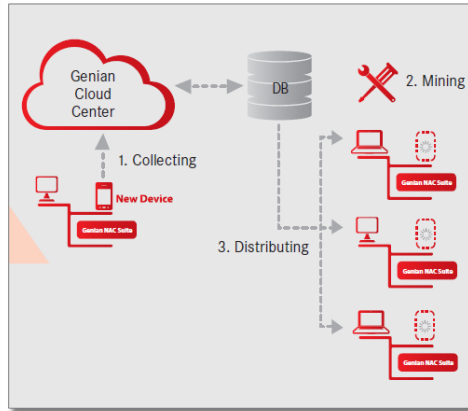
Genian NAC suite 특/장점

NAC 최고의 기술력을 바탕으로 한 안정성과 다양한 기능

플랫폼 DB 를 통한 장치 구분 및 플랫폼 자동 분류

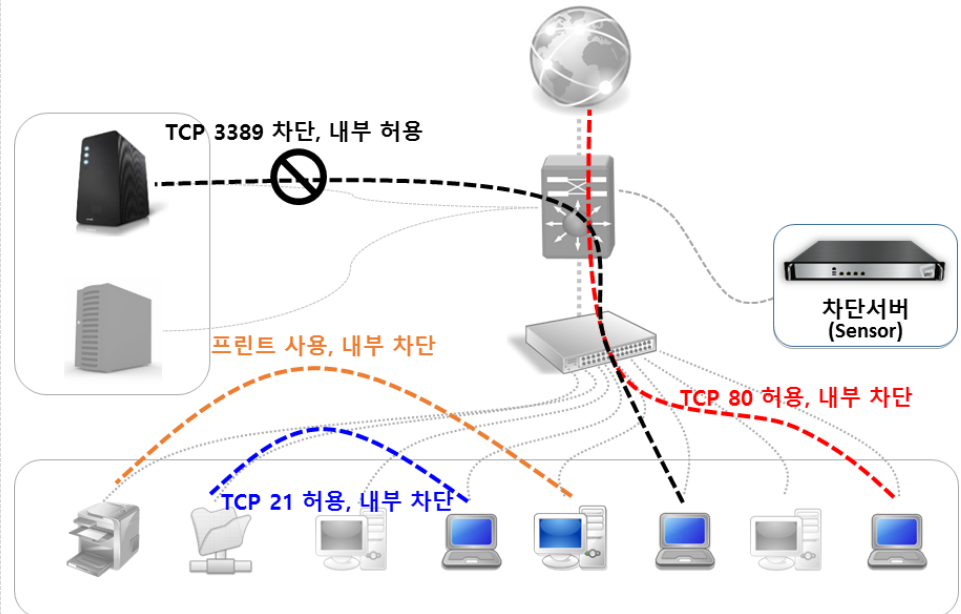
- Agent 설치 없이도 OS 버전, 모델명 등 자동 분류
- 신규 장치에 대한 cloud 형태의 자동 업데이트 기능 제공

172.29.20.83	40:80:5C:21:11:13	Microsoft Windows 7 Professional x64
172.29.20.84	BB:E8:58:3C:D0:34	Apple MacBook Pro
172.29.20.85	28:37:1E:14:F8	Apple MacBook Air
172.29.20.86	84:89:AD:88:8B:CE	Apple iPad
172.29.20.87	C4:12:F5:5B:94:E6	D-Link Wireless Router
172.29.20.89	C4:12:F5:5B:94:D6	D-Link International AP
172.29.20.90	BB:44:D9:62:EA:19	Apple iPhone
172.29.20.98	70:5A:0F:00:1B:6E	HP Officejet Pro 8100
172.29.20.99	F4:8D:04:50:1B:CD	Microsoft Windows 7 Professional
172.29.20.100	0C:8B:FD:EF:E2:5F	Microsoft Windows 10 x64
172.29.20.105	CC:3D:82:34:D2:EE	Microsoft Windows 10 Professional x64
172.29.20.106	D0:53:49:C6:01:15	Microsoft Windows 10 x64
172.29.20.107	10:4A:7D:70:38:A2	Microsoft Windows 7 Professional x64
172.29.20.109	CC:3D:82:34:D1:E0	Microsoft Windows 10 Professional x64
172.29.20.109	D6:CB:8A:84:D9:C1	Microsoft Windows 10 Professional x64
172.29.20.110	50:87:C3:05:C5:D5	Microsoft Windows 8.1 x64
172.29.20.111	F0:5B:7B:4D:A9:2F	Samsung Android Device
172.29.20.112	E4:FA:ED:20:9A:AF	Samsung Android Device
172.29.20.113	C8:FF:28:16:DE:51	Microsoft Windows 10
172.29.20.114	C4:12:F5:5B:95:03	D-Link International AP
172.29.20.115	74:27:EA:87:2F:D4	Microsoft Windows 7
172.29.20.116	C8:F7:33:1B:3E:4C	Microsoft Windows 10 x64
172.29.20.117	C8:F7:33:9A:C9:23	Microsoft Windows 10 x64
172.29.20.118	3C:15:C2:DA:6A:D6	Apple MacBook Pro
172.29.20.119	F4:F1:5A:30:FC:F6	Apple iPhone
172.29.20.120	C8:F7:33:D6:36:9D	Microsoft Windows 10 x64



방화벽 기반의 NAC

- Agent 와 무관한 네트워크 제어
- 방화벽 수준의 IP, Port, Protocol 제어 기능 제공

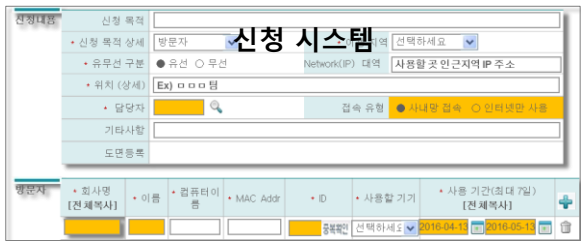


Genian NAC suite 특/장점

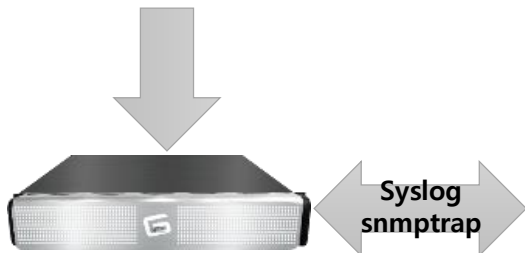
NAC 최고의 기술력을 바탕으로 한 안정성과 다양한 기능

타 시스템과의 유연한 연동을 통한 Security Eco system 구축

- Paloalto, FireEye, Trandmicro 기술 제휴를 통한 연동 완료
- Cisco ACI 연동 테스트 중
- NAC 자체 API 를 이용한 타 시스템과의 연동을 통한 자동화 구현

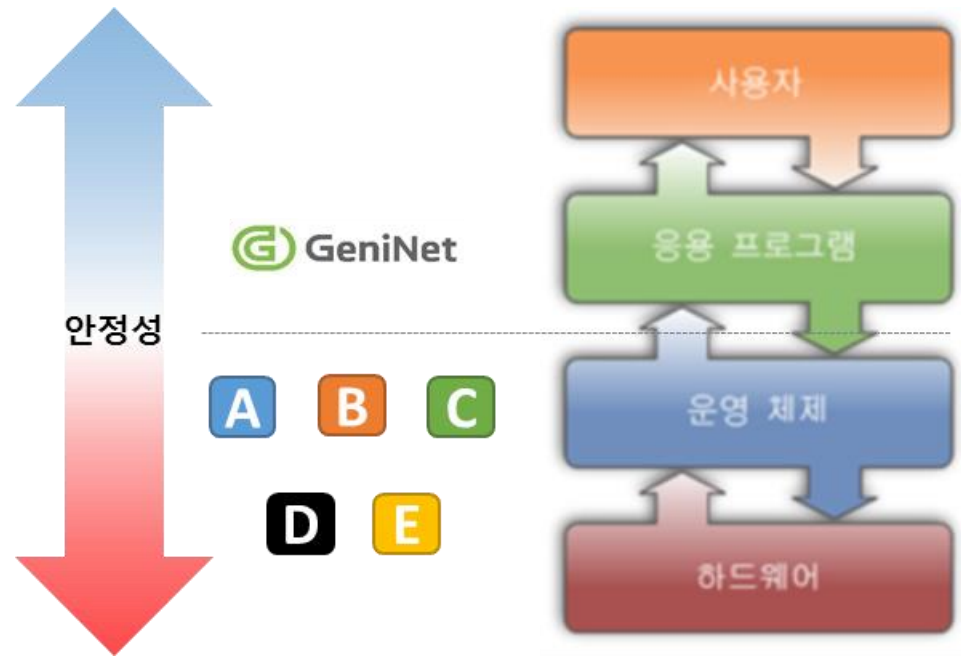


Genian API



Non-Driver 방식의 안정적인 Agent

- 운영체제(kernel) 레벨에서 동작하지 않아 OS 및 타 시스템과의 충돌 위험이 거의 없음



Genian NAC suite 특/장점

NAC 최고의 기술력을 바탕으로 한 안정성과 다양한 기능

Agent 의 기능 Plug-in 모듈화

- Agent 는 frame 에 불가
- 필요에 따라 Agent 에 기능을 추가/삭제 하는 구조
- 리소스 사용률 낮음
- 업그레이드 및 기능 추가 시 용이함



구분	플러그인명	버전	설명	
<input type="checkbox"/>	수집플러그인	IE보안옵션 제어	2.0.0.32311	IE의 보안옵션을 강제화 하는 기능을 제공합니다.
<input type="checkbox"/>	제어플러그인	PC전원 제어	2.0.0.32311	사용자 PC의 전원을 관리합니다.
<input type="checkbox"/>	수집플러그인	TCP세션검사	3.0.0.32311	주기적으로 TCP 세션을 수집하며 임계치상되는 세션수가 발견되면 네트워크 인터페이스를 차단합니다.
<input type="checkbox"/>	수집플러그인	WMI정보수집	4.0.0.32311	WMI를 통하여 시스템 정보를 수집합니다.
<input type="checkbox"/>	수집플러그인	검사만 수행	1.0.0.32311	액션에 설정된 검사 조건을 체크하는데 사용하는 플러그인입니다.
<input type="checkbox"/>	수집플러그인	게스트계정 제어	2.0.0.32311	윈도우즈 게스트 계정에 대한 사용여부를 제어합니다.
<input type="checkbox"/>	수집플러그인	네트워크 공유폴더	3.0.0.32311	네트워크에 공유된 폴더정보를 수집하여 일정시간 이상 공유되는 폴더를 제어합니다.
<input type="checkbox"/>	수집플러그인	네트워크정보 수집	2.0.0.32311	네트워크 인터페이스 정보와 탐지된 포트정보를 수집하여 노드정보에 표시합니다.
<input type="checkbox"/>	수집플러그인	모니터정보 수집	3.0.0.32311	로컬 컴퓨터에 연결되어있는 모니터에 대한 정보를 제공합니다.
<input type="checkbox"/>	수집플러그인	모양 및 개인설정	2.0.0.32311	윈도우 바탕화면, 화면보호기에 대한 설정 정보를 수집 및 제어합니다.
<input type="checkbox"/>	수집플러그인	무선랜제어	5.0.0.32448	무선 네트워크 인터페이스에서 탐지되는 무선 AP에 대한 정보를 제공하며 허용되지 않은 AP 연결을 제한합니다.

Geni Agent Plug-in

차단페이지 시뮬레이션 기능

- 관리자 콘솔을 통해 사용자의 차단 페이지 가상 확인 기능 제공



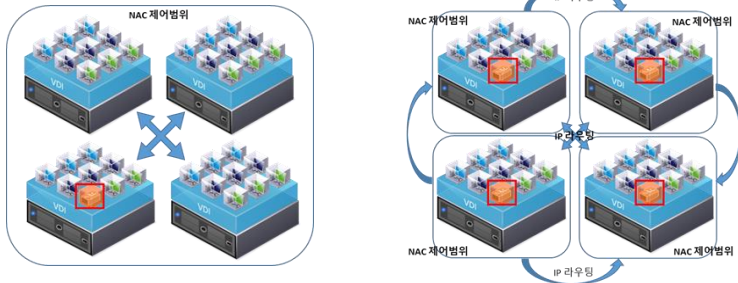
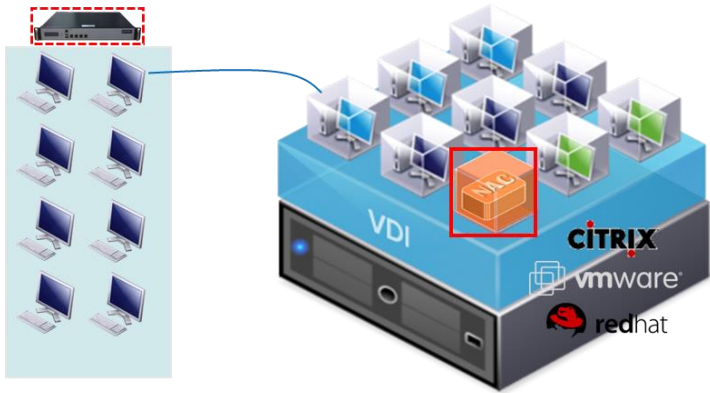
The screenshot shows the Genian NAC suite interface with a simulated captive portal page. The page displays user information: IP 주소: 172.29.109.123, MAC: 50-B7-C3-05-C5-D5, PC명: FOREST. It lists security features: DLP 설치, DRM, and 백신 파일. The interface also shows various system settings and user management options.

Genian NAC suite 특/장점

NAC 최고의 기술력을 바탕으로 한 안정성과 다양한 기능

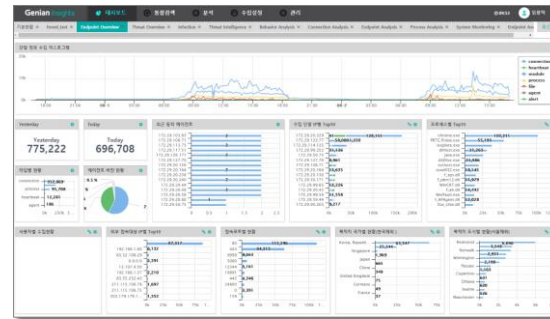
가상화 서버용 NAC SW

- 가상화 서버내 SW 형태의 NAC 설치를 통한 네트워크 제어
- 물리적인 PC와 동일한 제어 기능 제공

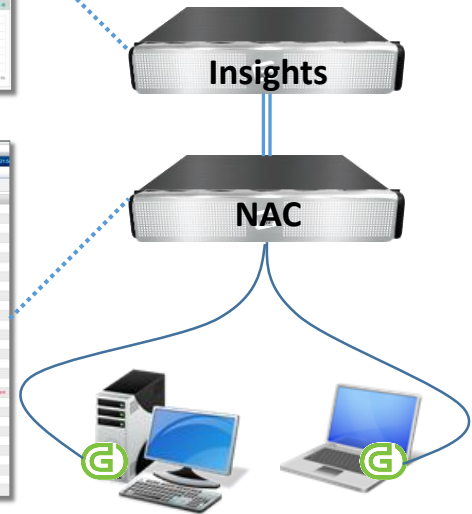


NAC 기반의 Insights 추가 확장 가능

- NAC 정보와 별도의 프로세스 기반 이상유무 탐지, 다양한 분석 시스템



IP 주소	장치명	상태	비고
192.168.1.1	SW-100	정상	관리자: admin
192.168.1.2	SW-101	정상	관리자: admin
192.168.1.3	SW-102	정상	관리자: admin
192.168.1.4	SW-103	정상	관리자: admin
192.168.1.5	SW-104	정상	관리자: admin
192.168.1.6	SW-105	정상	관리자: admin
192.168.1.7	SW-106	정상	관리자: admin
192.168.1.8	SW-107	정상	관리자: admin
192.168.1.9	SW-108	정상	관리자: admin
192.168.1.10	SW-109	정상	관리자: admin
192.168.1.11	SW-110	정상	관리자: admin
192.168.1.12	SW-111	정상	관리자: admin
192.168.1.13	SW-112	정상	관리자: admin
192.168.1.14	SW-113	정상	관리자: admin
192.168.1.15	SW-114	정상	관리자: admin
192.168.1.16	SW-115	정상	관리자: admin
192.168.1.17	SW-116	정상	관리자: admin
192.168.1.18	SW-117	정상	관리자: admin
192.168.1.19	SW-118	정상	관리자: admin
192.168.1.20	SW-119	정상	관리자: admin
192.168.1.21	SW-120	정상	관리자: admin
192.168.1.22	SW-121	정상	관리자: admin
192.168.1.23	SW-122	정상	관리자: admin
192.168.1.24	SW-123	정상	관리자: admin
192.168.1.25	SW-124	정상	관리자: admin
192.168.1.26	SW-125	정상	관리자: admin
192.168.1.27	SW-126	정상	관리자: admin
192.168.1.28	SW-127	정상	관리자: admin
192.168.1.29	SW-128	정상	관리자: admin
192.168.1.30	SW-129	정상	관리자: admin
192.168.1.31	SW-130	정상	관리자: admin



가시성 (Visibility)

내부 네트워크 내의 모든 단말기 정보 수집, 인사시스템 연동을 통한 IP 실명 확인

위험	동작	IP주소	MAC주소	정책	호스트명(이름)	플랫폼	인증사용자	위치	스위치,포트	마지막 동작시각
		192.168.0.2	AC:E0:10:0B:39:E5		BATU	Microsoft Windows 10 Home		Guest-Net (192.168.0 /24)		2015-10-24 12:59:22
		172.29.20.163	18:67:B0:C5:A6:22		김상환	Microsoft Windows 8.1		사업부-20	Technical_Support 1/24	
		192.168.0.45	D8:1D:72:DA:DD:6E		JunSeoks-6	Microsoft Windows		Guest-Net (192.168.0 /24)		
		172.29.50.34	00:15:F2:6A:AA:41					연구소-50		2015-10-01 12:31:42
		172.29.20.91	E8:03:9A:E7:A7:87		JAESUNGLYU-PC	Microsoft Windows 7 Home Premium		사업부-20	BackBone Gi1/0/47	2015-10-30 11:44:57
		172.29.100.195	44:8A:5B:F4:49:1A			Linux		인프라보안기술부-100	Technical_Support 1/24	
		172.29.101.254	00:1B:8F:37:30:5C		BackBone	Cisco Catalyst 3750 Switch		인프라보안기술부-101	Technical_Support 1/24	
		172.29.100.20	00:30:48:D6:8E:57		메인센터	GeniNetworks Genian NAC		인프라보안기술부-100	Technical_Support 1/24	
		172.29.90.19	00:30:48:D6:8E:57		메인센터	GeniNetworks Genian NAC		연구소-90	Technical_Support 1/24	
		172.29.50.139	6C:29:95:0E:91:F6			Microsoft Windows 10 x64		연구소-50	cisco-lab01 Gi1/0/10	2015-10-29 13:04:31
		172.29.50.139	24:F5:AA:C2:B9:41		DORIPARK-WINPC	Microsoft Windows 10 x64		연구소-50	cisco-lab01 Gi1/0/10	2015-10-30 14:10:19
		172.29.20.114	6C:29:95:0E:91:F6		DORIPARK-WINPC	Microsoft Windows 10 x64		사업부-20	cisco-lab01 Gi1/0/10	
		172.29.250.15	6C:29:95:0E:91:F6		DORIPARK-WINPC	Microsoft Windows 10 x64		C-172.29.50.150	cisco-lab01 Gi1/0/10	
		172.29.20.180	00:00:00:00:02:6F		YOONA	Microsoft Windows 8.1		사업부-20	Technical_Support 1/24	2015-10-30 11:41:18
		172.29.50.62	6C:62:6D:2C:2B:95		LBT-00_AIVD	Microsoft Windows 7 Professional		연구소-50	Gi1/0/9	
		172.29.90.71	08:00:27:26:06:51			Linux		연구소-50	Gi1/0/22	
		172.29.50.20	00:30:48:D6:8E:56		메인센터	GeniNetworks Genian NAC		연구소-90	BackBone Gi1/0/6	
		172.29.20.188	AA:AA:AA:AA:AA:AA		smilm-PC	Microsoft Windows 8.1		사업부-20	Technical_Support 1/24	2015-10-29 18:09:30
		172.29.404.497	AA:AA:AA:AA:AA:AA		SMLIM-PC	Microsoft Windows 8.1		인프라보안기술부-101	Technical_Support 1/24	2015-10-29 17:42:27
		172.29.404.406	00:0C:29:C2:D9:D0		smilm	Microsoft Windows		인프라보안기술부-101	Technical_Support 1/24	2015-10-11 18:44:21
								인프라보안기술부-100	Technical_Support 1/24	2015-10-13 15:38:15
		172.29.20.111	6C:29:00:00:00:00		THKIM	Microsoft Windows 8.1		사업부-20	Technical_Support 1/24	
		172.29.99.170	FF:FF:FF:FF:FF:FF			NAT장치(공유기)		사업부-20	cisco-lab01 Gi1/0/10	2015-08-30 16:16:05
								C-172.29.50.150		

신규 플랫폼 탐지 및 정확도를 높이기 위한 지속적인 관리 및 업데이트 지원

• 자체 CLOUD 서비스를 통한 단말기 상세 정보 제공

- 1) 실 네트워크에서 단말 정보 수집
- 2) CLOUD에서 정제/가공
- 3) NAC 에 재 배포(DB Update)
- 4) 새로운 단말 인식 및 분류

• 장치분류 DB

PC, Server, Printer, Switch, 보안 장비, Voip, Mobile 등 장치 자동 분류

• 플랫폼 DB

장치에 대한 OS 및 버전, 모델명 등 장치에 대한 상세 분류를 할 수 있는 전문적인 플랫폼 DB
현재 20,000여 이상의 단말을 정보 CLOUD를 통하여 매월 100 건 이상 Update

IP 실명제

위험	IP	동작	IP주소	MAC주소	정책	호스트명	플랫폼	인증	위치	스위치포트	연결방식
위험 행위 노드	IP정책 위반 노드	UP/Down	IP주소	MAC주소	적용되어 있는 정책	PC이름	종류 / 기기 명칭	인증된 사용자 ID	현재 노드가 탐지된 위치	SNMP연동	Agent 및 AP 탐지

가시성 (Visibility)

PC 내의 다양한 정보 제공

모든 단말기의 정보를 제공하며, Agent 설치 시 추가 정보 확인 가능

기본정보 장비정보 네트워크정보 이력관리 IP관리 정책 정책현황 Agent 미 설치 단말 정보

기본정보 장비정보 시스템정보 네트워크정보 소프트웨어정보 패치정보 이력관리 IP관리 정책 정책현황 Agent 설치 단말 정보

IP 주소

이름

도메인

노트타입

플랫폼

장비 위치

접속AP

연결방식

마지막 동작시각

최초 등록

인증사용자

현재 인증상태

설명

장비명

장비설명

마더보드 정보

마더보드 제

메모리 정보

저장장치 정보

장치명

운영체제 정보

인터페이스 정보

연결방식

공유 정보

사용자계정 정보

사용자

화면보호기 정보

사용자

GPI 점수

모니터 정보

모뎀

프린터 정보

트래픽 정보 (프로토콜)

트래픽 정보 (목적지)

목적지

탐지된 AP 목록

SSID

Sentry#AP 44:AD:D

TCP 세션 정보 (평균값)

세션 전체

탐지된 서비스 목록

구분

열린포트 정보

닫지

백신 정보

AhnLab V3 Internet Security 9.0

Windows Defender

소프트웨어 정보

AhnLab Online Security

AhnLab V3 Internet Security

Apache Tomcat 9.0 Tomcat9

Chrome

ColorEngine

Dolby Digital Plus Home Th

EditPlus

ELAN Touchpad driver X64

Genium GPI

HeidiSQL

HP Officejet Pro 8640 기본

HP Officejet Pro 8640 드

HP Update

i.R.I.S. OCR

INISafe SFilter 7.2 (SFilter v

INISafeWeb 6.4

Intel(R) Dynamic Platform a

Intel(R) Management Engin

Intel(R) Processor Graphics

패치명

- 1 Windows 8, 8.1, 10 및 Windows Server 2012, 2012 R2 x64 Edition용 Win
- 2 x64 기반 시스템용 Windows 10 Version 1511 누적 업데이트(KB3172985)
- 3 Microsoft Word 2013용 보안 업데이트(KB3115292) 32비트 버전
- 4 Microsoft Excel 2013용 보안 업데이트(KB3115262) 32비트 버전
- 5 Microsoft Outlook 2013용 보안 업데이트(KB3115259) 32비트 버전

시간	프로그램	그룹	관리상태	IP	MAC
2016-06-03 08:53:59	알림	네트워크정보	172.29.117.4	172.29.117.51	98.83.89.1A.91.CB
2016-06-03 08:52:52	알림	시스템정보	172.29.117.4	172.29.117.51	98.83.89.1A.91.CB
2016-06-03 08:52:52	알림	시스템정보	172.29.117.4	172.29.117.51	98.83.89.1A.91.CB
2016-06-03 08:52:52	알림	정책	172.29.117.4	172.29.117.51	98.83.89.1A.91.CB
2016-06-03 08:52:52	알림	정책	172.29.117.4	172.29.117.51	98.83.89.1A.91.CB
2016-06-03 08:52:52	알림	인증	172.29.117.4	172.29.117.51	98.83.89.1A.91.CB
2016-06-03 08:52:48	알림	에이전트액션	172.29.117.4	172.29.117.51	98.83.89.1A.91.CB
2016-06-03 08:52:45	알림	에이전트액션	172.29.117.4	172.29.117.51	98.83.89.1A.91.CB
2016-06-03 02:01:23	알림	정책	172.29.117.4	172.29.117.51	98.83.89.1A.91.CB
2016-06-03 02:01:23	알림	정책	172.29.117.4	172.29.117.51	98.83.89.1A.91.CB

노드정책

기술부 정책(테스트)

제어정책

정책명

기본정책

노드그룹

노드그룹

모든노드

PC

백신 동작

백신 미동작

백신 실시간검사 미사용

백신 실시간검사 사용

백신 업데이트 만족

백신 업데이트 불만족

Microsoft Windows

동작노드

컴퓨터이연스 위반노드

에이전트 설치노드

(그룹) 인프라보안기술부

Bios 수집 그룹

(그룹) 국보연 테스트_BIOS_Password

(그룹) 국보연 테스트_BIOS_정보수집

(확인) local

위험감지

위험감지

에이전트액션 수행결과

에이전트액션

006) 무선랜 정보수집

007) 모니터정보 수집

008) 프린터정보 수집

가시성 (Visibility)

Dashboard 를 통한 다양한 통계, 상태 등의 현황 파악 용이

대시보드는 Genian NAC suite 의 메인 페이지로 관리자가 관심있는 항목에 대해 간단하고 가시성 있게 정보를 표현하여, 상황파악을 쉽게 할 수 있도록 함

관리자가 도입 솔루션의 기능 전반을 손쉽게 활용하여, 도입 장비의 가치를 높일 수 있도록 함

The image displays the Genian NAC suite dashboard and a configuration window. The dashboard (labeled 1) features several widgets: a large '100%' status indicator, a pie chart for '무선랜 접속AP 현황(Top 10)', a gauge for '노드 사용자 인증률(Gauge)', a line graph for 'UP 노드 평균용량(치트)', a table for '노드 분류', and a table for '에이전트 설치현황'. The configuration window (labeled 2) is titled '위젯 추가' and shows a list of widgets (labeled 3) such as '위젯 카테고리', '네트워크(6)', '무선랜 접속AP Top 10 현황을 표시합니다.', and '무선랜 그룹 비율'. A legend at the bottom identifies the components: 1 TAB (관리 TAB), 2 설정 (전반적인 위젯 기능), and 3 위젯 (위젯 추가 화면).

분류 (Classify)

다양한 조건의 그룹 별 분류, 정보 확인 기능

현황 & 필터

- 노드정책
 - insights 개발 1 0%
 - 기술연구소 정책 24 2%
 - 기술부 정책(테스트) 12 1%
 - WAA SUP사업부 정책 13 1%
 - 인프라보안사업부 정책 0 0%
 - 경영관리실 정책 8 1%
 - 기본정책 1154 95%
- 제어정책
- 노드그룹
- 위험감지
- 위험노드
- 네트워크 그룹
- 서비스
 - PC 310 24%
 - 기타 191 15%
 - 보안장비 182 14%
 - 서버 108 8%
 - VOIP 103 8%
 - 모바일 100 8%
 - 네트워크장비 84 7%
 - 센서 70 5%
 - 미분류 49 4%
 - 무선결속장비 48 4%
 - 스위치 24 2%
 - 프린터 14 1%
 - 센터 1 0%
- 부서(노드그룹)
- 부서(인증사용자)
- 인증사용자
- 노드타입
 - 모바일 100 8%
 - 네트워크장비 84 7%
 - 센서 70 5%
 - 미분류 49 4%
 - 무선결속장비 48 4%
 - 스위치 24 2%
 - 프린터 14 1%
 - 센터 1 0%
- 노드상태
 - 동작상태 49 4%
 - 인증상태 48 4%
 - NAT 24 2%
 - AP Device 14 1%
- 클라우드
- IP관리
- 에이전트
 - 운영제제
 - 소프트웨어
 - IE버전
 - 하드웨어
 - 패치
 - 패치상세
 - 액션상세
 - 액션수행결과
 - 노드세션
 - 트래픽
 - 태그
 - 연결방식

노드정책 적용 현황

insights 개발	1	0%
기술연구소 정책	24	2%
기술부 정책(테스트)	12	1%
WAA SUP사업부 정책	13	1%
인프라보안사업부 정책	0	0%
경영관리실 정책	8	1%
기본정책	1154	95%

세이정책 적용 현황

HDH_netctrl_test	0	0%
제외하루	931	77%
에이전트미설치자단	12	1%
미인증자단	75	6%
GPI 미설치자단	0	0%
기본정책	195	16%

서비스 적용 현황

DHCP 서버	67
DNS 서버	9
FTP서버	28
Secure 웹서버	211

노드 타입 (Pie)

연결방식 현황

유선LAN	347
무선LAN	114
알수없음	823

전체노드 / 플랫폼 현황

플랫폼	수량	비율
Microsoft Windows	245	20%
GenNetworks Genian NAC	126	10%
Cisco Networking Device	79	7%
Microsoft Windows 10 x64	68	6%
Apple iPhone	40	3%
Microsoft Windows 10 Professional x64	35	3%
Linux	32	3%
GenNetworks Genian GPI	30	2%
Microsoft Windows 7 Professional	25	2%
D-Link International AP	24	2%
Moimstone IP255 VOIP Phone	23	2%
Microsoft Windows 8.1 x64	22	2%
Cisco Catalyst 2960 Switch	21	2%
Microsoft Windows	21	2%
MOIMSTONE IP255S 1.30 510	21	2%
Apple MacBook Pro	20	2%
Microsoft Windows 7 Professional x64	20	2%
Stonehenge IP255-S 1.30 236	20	2%
Apple Device	17	1%

전체노드 / 하드웨어 현황

자산현황 - CPU

CPU 제조사	수량	비율
INTEL	76	92%

자산현황 - 메모리

메모리 크기	수량	비율
513MB-1024MB	4	1%
1025MB-2048MB	4	5%
2049MB-4096MB	20	24%
4097MB-8192MB	33	40%
8193MB-OVER	22	27%

자산현황 - 모니터

모니터 크기	수량	비율
0~9"	1	1%
10~13"	36	27%
14~16"	11	8%
18"	1	1%
20"	1	1%
21"	26	20%
23"	46	35%
24"	8	6%
27~29"	1	1%
30~OVER	1	1%

자산현황 - 저장장치

저장장치 크기	수량	비율
11GB-20GB	1	1%
21GB-40GB	3	4%
41GB-60GB	1	1%
81GB-100GB	3	4%
101GB-150GB	11	13%
151GB-200GB	3	4%
201GB-250GB	15	18%
301GB-500GB	12	14%
501GB-750GB	3	4%
751GB-1024GB	7	8%
1025GB-2048GB	15	18%
2049GB-OVER	4	5%

자산현황 - 로컬 프린터 (Top 10)

프린터명	수량	비율
Microsoft Shared Fax Driver	74	20%
Send to Microsoft OneNote 15 Driver	60	17%
Microsoft XPS Document Writer v4	55	15%
Hancom PDF	49	14%
Microsoft Print To PDF	40	11%
Microsoft XPS Document Writer	19	5%
Canon MB2300 series Printer	16	4%
Canon MB2300 series FAX	16	4%
Adobe PDF Converter	6	2%
HP Officejet Pro 8100	4	1%

통제 (Control)

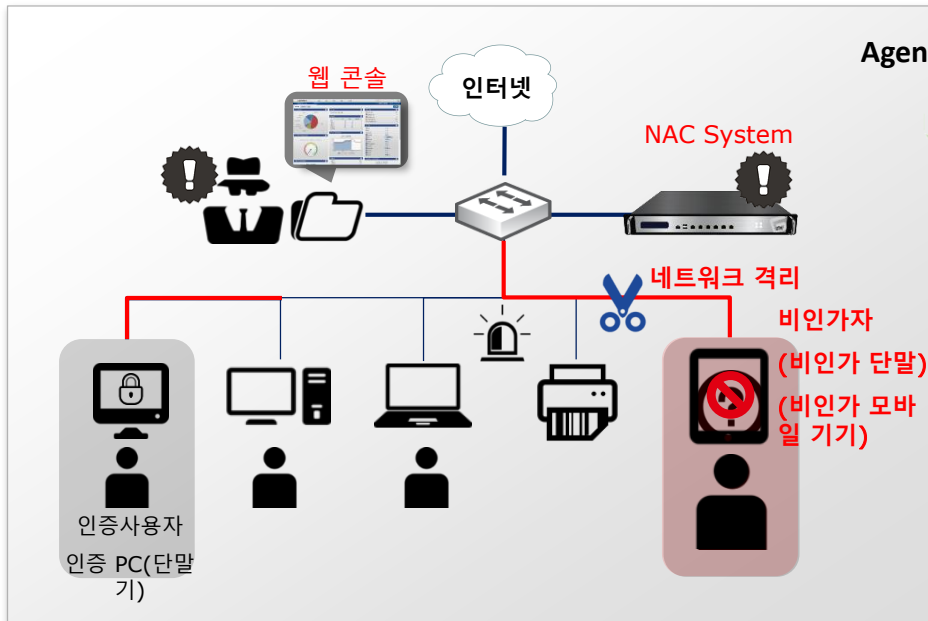
네트워크 통제(Network Control)

전용 장비를 이용한 네트워크 통제 기능

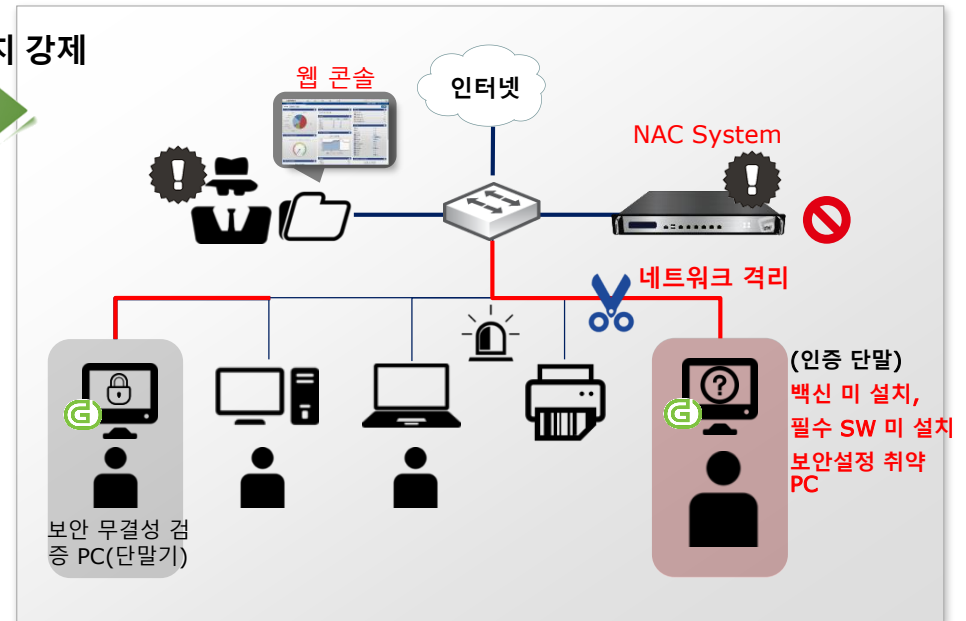
- IP 관리통제
- 미 인증 통제
- 방화벽 수준의 IP, Port, Protocol 기반 통제
- 단말기 분류에 따른 통제

Agent 설치 후 전용 장비를 이용한 네트워크 통제 기능

- 필수 SW 미 설치 단말기 네트워크 통제 (설치 유도)
- 보안 무결성 상태에 따른 네트워크 통제



Agent 설치 강제



통제 (Control)

PC 정보 수집 및 설정에 대한 통제 기능

PC 내의 정보 수집과 장치에 대한 On/Off 기능

보안 설정에 대한 교정 기능

PC 내의 보안 무결성 상태에 따른 네트워크 제어 기능



유연한 차단페이지 구성(HTML)

방화벽과 같이 안내 없는 차단이 아닌 차단 사유 설명 및 조치 방안에 대한 안내페이지 제공

- 사용자가 조치할 수 있도록 별도의 가이드 페이지 및 다용도 Link 제공
- 안내 메시지 등 문구 지정 가능(HTML 지원)
- 다중 페이지 지원(A 정책용 차단 페이지, B 정책용 차단 페이지 별도 지정 가능)



Genian NAC suite 구성도

1. Policy Center & Console (정책서버)

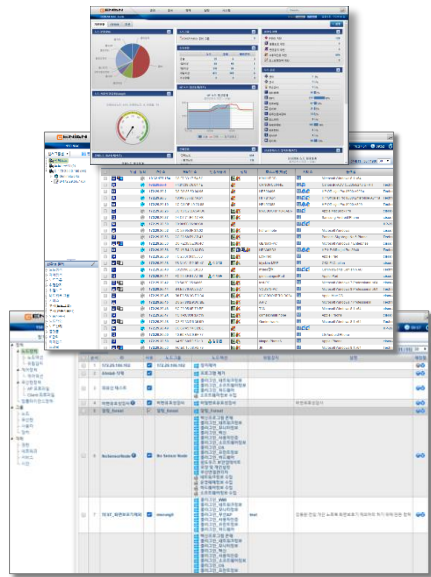
유선과 무선을 아울러 통합관리하고 내부 보안을 강화할 수 있도록 지원

2. Net-Sentry

유선/무선 단말에 대한 정보를 수집하고 네트워크통제 수행

3. Agent

Agent 설치 단말에 대한 보안상태를 점검
(Agent 설치를 권장하나, 필수가 아닌 선택 사항이며, 상황에 맞게 설치/미설치 형태로 운영 가능)



1. 정책서버

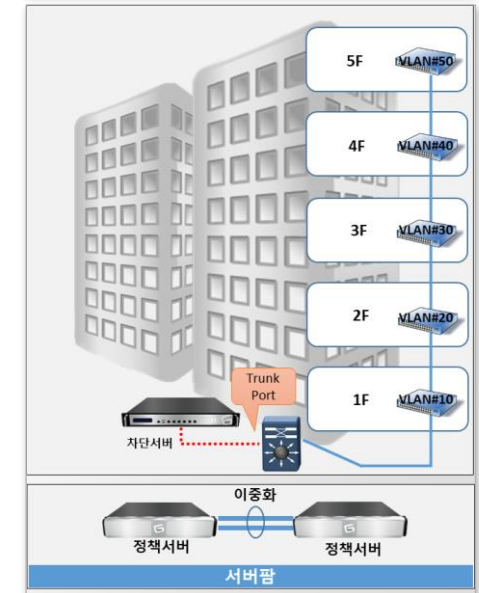
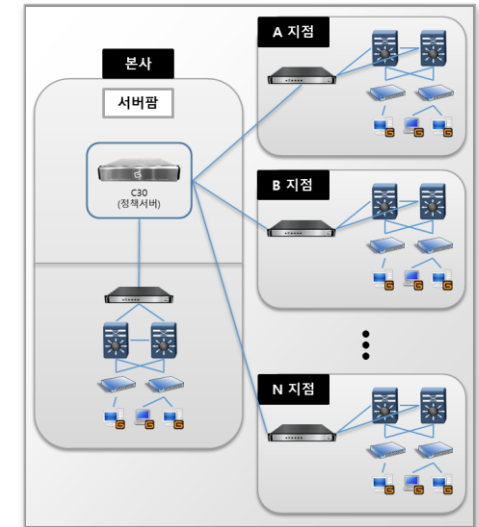
- 보안정책 수립
- 단말 관리
- 현황 및 이력관리
- 자체OS 및 이중화 지원

- 사용자 단말 인증
- 유선 단말 정보 수집
- 유.무선 단말 차단
- 802.1q 지원

2. 차단서버

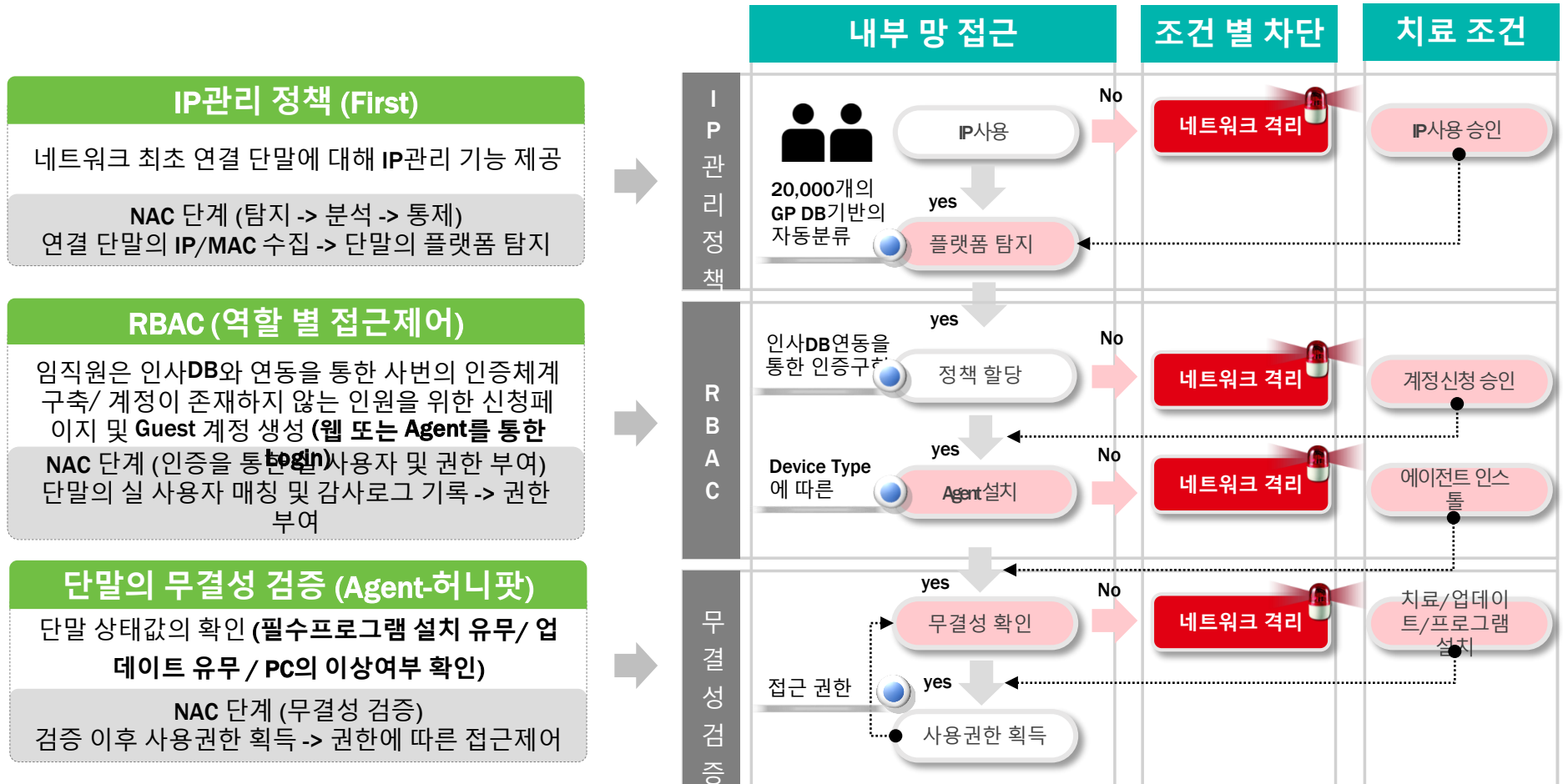
3. Agent

- PC무결성 점검
- PC 패치 및 자산관리
- Ad-hoc, 우회경로 차단



Genian NAC suite 주요 프로세스

내부 네트워크 사용 시 단계적 검증 Process 성립

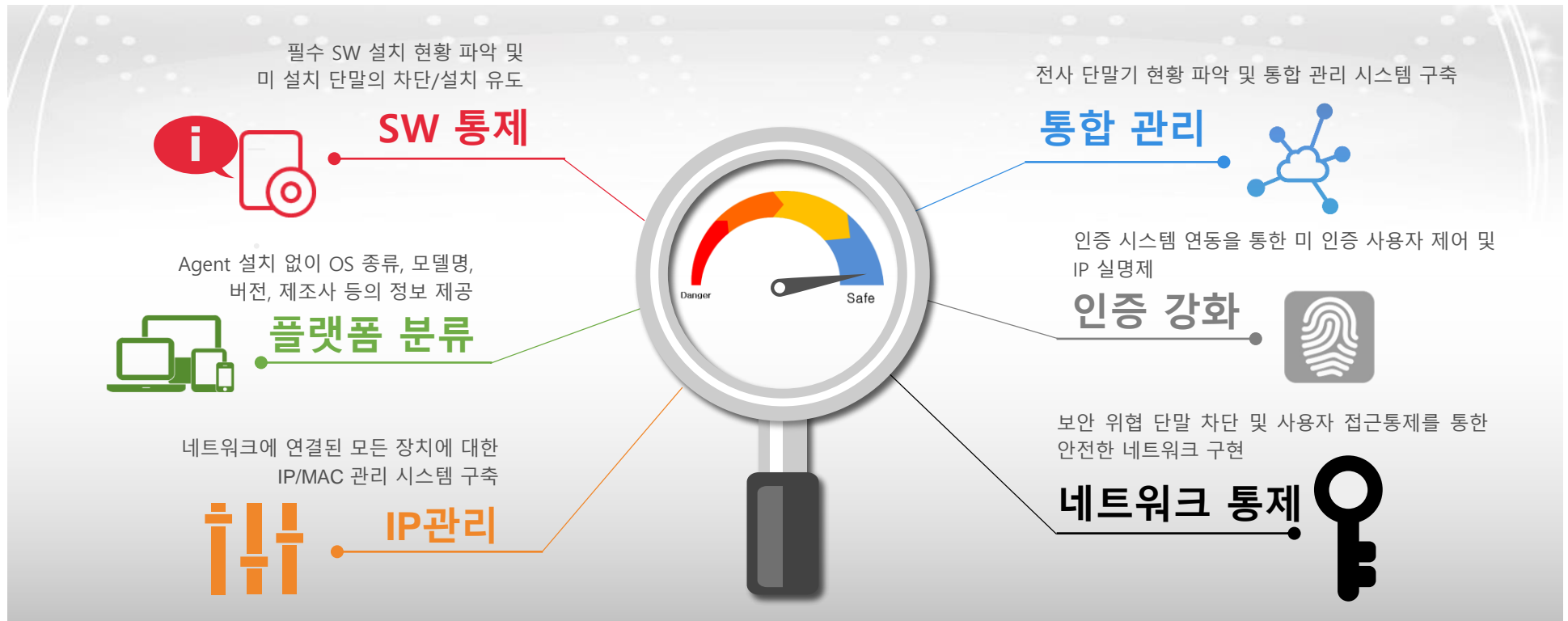


Genian NAC suite 도입효과

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





지니네트웍스(주) 회사소개

회사개요

내부보안 국내 최고의 네트워크 접근제어 시스템 Genian NAC suite 개발사

1

시장 점유율 1위

2015년 약 50% 점유율로 압도적인
시장 점유율

10

연구개발 10년(2005~)

2005년 국내 최초 네트워크 접근제어
시스템 개발 후 10년 넘는 연구 개발

100

매출 100억 돌파(2014년)

2014년 네트워크 접근제어 시스템
시장에서의 최초 100억 매출 돌파



1,000

도입 고객사

2005년 부터 약1,000 곳의 고객사 구축

10,000

40 여 곳의 10,000 노드 이상 구축

10,000 노드 이상의 대형 고객사
구축

100,000

단일 최대 100,000 노드 이상의 구성 가능

단일 최대 100,000 노드 이상의 구성이 가능한
성능 구현



회사개요

고객과 함께 좋은 가치를 만들어 갑니다. 행복한 꿈을 이뤄가는 기업, 지니네트웍스



회 사 명	지니네트웍스 (주)
대 표 이 사	이 동 범
설 립 일	2005년 01월 07일
자 본 금	5억
주 요 사 업	네트워크 보안 솔루션 개발/판매, 보안감사(audit) 솔루션 개발/판매
임 직 원 수	97명 (17년 01월 현재)
협 력 사	론스텍(총판), 대신정보통신(총판) 등 약 30개사
주 소	경기도 안양시 동안구 시민대로 361 에이스평촌타워 803호
홈 페이지	http://www.geninetworks.com/

핵심 경쟁력

국내 최고의 기술력을 바탕으로 내부 보안시장을 선도 하는 지니네트웍스

시장지배력



네트워크 접근제어
시장
50% 이상 점유

누적 약1,000 곳의
고객사 보유



검증된 기술력



국내 최초 네트워크
접근제어 개발 및 출
시

내부 보안분야
국내 시장 기술선도

전문성



최고의 보안전문
인력 보유

내부 보안사이클 운
영
솔루션 라인업 보유

내부 보안(Internal Security) 전문기업 지니네트웍스

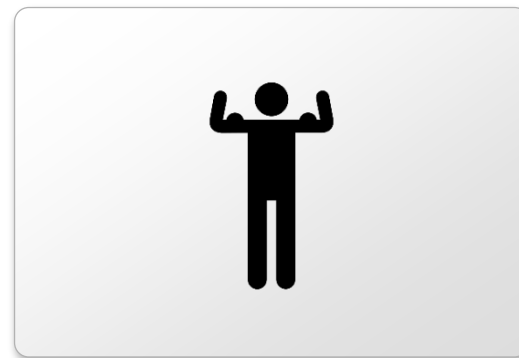
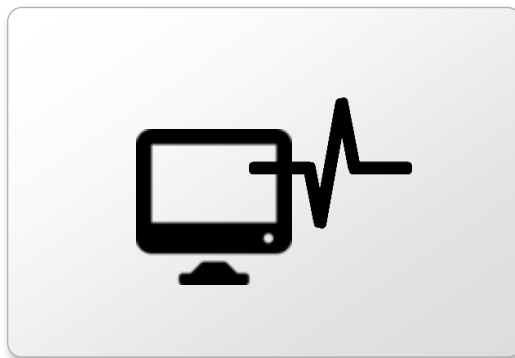
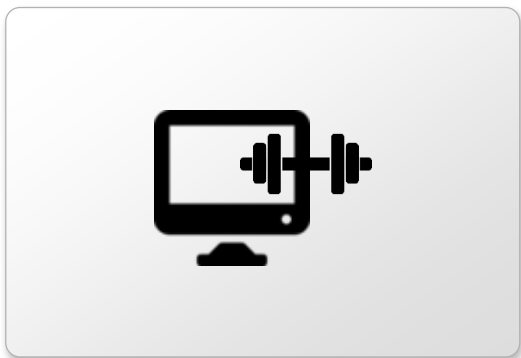
체력강화

정기검진

생활습관 개선

Genian NAC suite Suite
(네트워크 접근 제어)

Genian 내PC지키미
(보안수준 진단)



주요 고객사

공공기관



금융분야



일반기업





Thank you!