

통합 보안 플랫폼 기업, 지니언스

Genian NAC

(On-premise/Cloud)



Table of Contents

01. 배경 및 필요성

02. Genian NAC 제품 소개

03. 사용자 스토리

04. 주요 고객사

01.

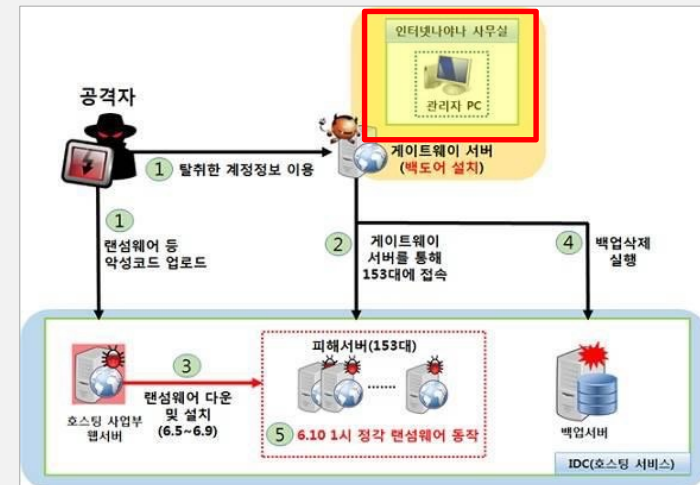
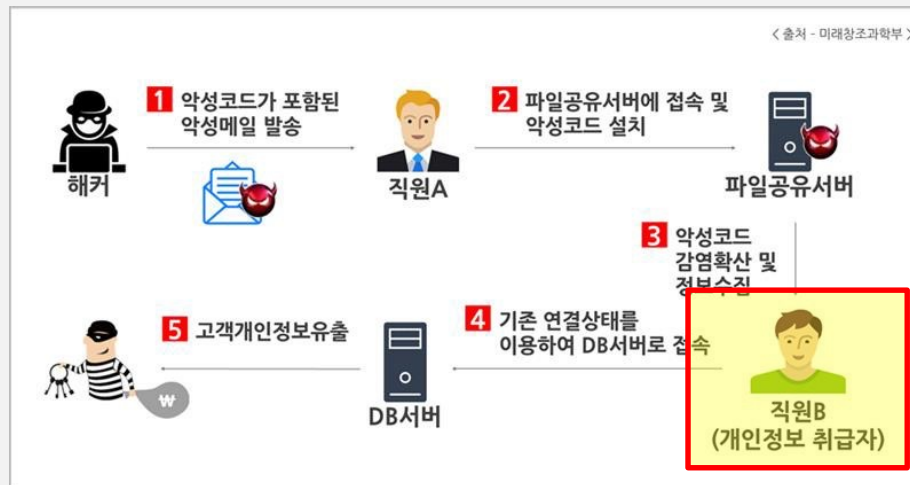
배경 및 필요성

“전통적인 방법의 기술 유출과 지능적인 해킹”

대표적 공격 종류 3가지

1. 기술 유출 및 외부 공격 위험 : 외부에서 접근 가능한 장치들이 회사 내부에 접근 할 수 있는 환경
2. 장치 인증 및 소셜 엔지니어링 : 인증되지 않는 장치 및 사용자가 내부에 접근 / 청탁을 통한 내부 관계자 접근
3. 악성 소프트웨어 감염 : 보안패치가 적용되지 않은 장치의 사용으로 취약점에 노출된 장치인한 정보 유출 가능성 높음

외부 위협과 내부 관계자 및 내부 보안관리 부재로 인한 피해 증가



ISMS 기준 대비 NAC 도입 타당성

ISMS-P 인증기준 안내서 (2023.10.31 기준)



ISMS-P 법적근거



- 정보통신망 이용촉진 및 정보보호에 관한 법률 제47조
- 정보통신망 이용촉진 및 정보보호에 관한 법률 시행령 제47조~제54조
- 정보통신망 이용촉진 및 정보보호에 관한 법률 시행규칙 제3조
- 개인정보보호법 제32조의2
- 개인정보보호법 시행령 제34조의2~제34조의8
- 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시

외부자 보안 보호대책 요구사항 2.10.6 (업무용 단말 기기 보안)

보안시스템 접근통제 정책(사용자 인증, 관리자 단말 IP / MAC)

정보자산 분류 관리체계 수립 및 운영 1.2.1 (정보자산 식별 세부 설명)

정보자산의 분류기준을 수립, 자산 식별하여 목록 관리

물리적 보안 보호대책 요구사항 2.5 (인증 및 권한 관리)

정보시스템 및 개인정보 시스템 접근 시 보호대책 마련

접근통제 보호대책 요구사항 2.6 (접근통제)

업무상 중요 정보가 비인가자에게 유출되지 않도록 보호대책 마련

무선통신통제 보호대책 요구사항 2.6.5 (무선 네트워크 접근 통제)

무선 네트워크 사용하는 경우 사용자 인증 및 통제 보호대책 마련

개인정보보호위원회 개인정보의 안정성 확보 조치 기준

- 제6조(접근통제)** ① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.
1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol) 주소 등으로 제한하여 인가받지 않은 접근을 제한
 2. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응

방송통신위원회 정보보호 관리지침

- 제18조(정보시스템 보안관리)** ① 각급기관의 장은 정보시스템(정보통신망을 포함한다)의 효율적인 보안관리를 위하여 정보시스템별로 관리책임자(이하 '시스템관리자'라 함)를 각각 서버·PC 정보통신장비 등 정보시스템이 비인가자에게 허용되지 않도록 보안기능을 설정하여야 한다.
- ② 시스템관리자는 보안도구를 이용하여 정보시스템의 보안취약점을 진단하여야 하며, 시스템 접속시 다음 각 호의 사항이 자동 저장되도록 하여야 한다.
1. 서버 접속일시, 접속자 및 접속방법 등 정보통신망 접근기록(1차)
 2. 전산자료 열람 출력 등에 대한 사용자, 일시, 자료제목 등 접근기록(2차)
 3. 시스템관리자는 다음 각 호와 같이 자동 수록된 접근자료(Log Data)를 관리하여야 한다.
1. 접근자명은 접속의 성공여부와 상관없이 기록 유지

의료기관 개인정보보호 가이드 라인 ④ 최소 3개월 이상 보관(백업자료 포함) 및 외부유출 방지를 위한 보호대책 감구

- 기술적 조치**
- ▶ 접근 권한의 제한·관리
 - ▶ 접근통제 시스템 설치 및 운영
 - ▶ 개인정보 암호화
 - * 주민번호를 보관 시에는 반드시 암호화하여야 함
 - ▶ 접속기록의 보관 및 위·변조 방지
 - ▶ 보안 프로그램의 설치·운영
 - ▶ 관리용 단말기의 안전조치

ISMS 인증기준항목별 NAC 대응사항

영역	분야	적용 여부		NAC 활용/대응 항목
		ISMS	ISMS-P	
1. 관리체계 수립 및 운영 (16개)	1.1. 관리체계 기반 마련	○	○	
	1.2. 위험 관리	○	○	1.2.1 정보자산 식별
	1.3. 관리체계 운영	○	○	
	1.4. 관리체계 점검 및 개선	○	○	
2. 보호대책 요구사항 (64개)	2.1. 정책, 조직, 자산 관리	○	○	
	2.2. 인적 보안	○	○	2.2.3 보안서약
	2.3. 외부자 보안	○	○	2.3.2 외부자 계약 시 보안
	2.4. 물리 보안	○	○	2.4.7 업무환경 보안
	2.5. 인증 및 권한관리	○	○	
	2.6. 접근통제	○	○	2.6.1 네트워크 접근 2.6.5 무선 네트워크 접근 2.6.6 원격접근 통제* 2.6.7 인터넷 접속 통제*
	2.7. 암호화 적용	○	○	
	2.8. 정보시스템 도입 및 개발 보안	○	○	
	2.9. 시스템 및 서비스 운영관리	○	○	
	2.10. 시스템 및 서비스 보안관리	○	○	2.10.6 업무용 단말기기 보안 2.10.7. 보조저장매체 관리
	2.11. 사고 예방 및 대응	○	○	
	2.12. 재해복구	○	○	
3. 개인정보 처리 단계별 요구사항 (22개)	3.1. 개인정보 수집 시 보호조치	-	○	
	3.2. 개인정보 보유 및 이용 시 보호조치	-	○	
	3.3. 개인정보 제공 시 보호조치	-	○	
	3.4. 개인정보 파기 시 보호조치	-	○	
	3.5. 정보주체 권리보호	-	○	

※ 2023년 11월 23일 기준

1.2.1 정보자산 식별

- 조직의 업무특성에 따라 정보자산 분류 기준 수립 및 모든 자산 식별•분류

2.2.3 보안 서약 / 2.3.2 외부자 계약시 보안

- 정보자산 취급 및 접근권한이 부여된 임직원에게 대해 법규와 비밀 유지의 고지 및 정보보호 서약
- 중요정보 및 개인정보 처리 관련 서비스를 위탁 선정하는 경우 정보보호 개인정보보호 요구사항 식별 및 관련 내용을 계약서에 명시하고 절차 마련

2.4.7 업무환경 보안

- 문서고, 공용PC, 복합기 파일서버 등 공용사용 시설 사무기기에 대한 보호, 업무환경을 통해 비인가자에게 노출 유출 되지않게 클린데스크 정기점검 대책 수립 및 이행

2.6.1 네트워크 접근 / 2.6.5 무선 네트워크 접근

- 네트워크에 대한 비인가 접근을 통제하기 위해 IP관리, 단말인증 관리 절차 수립•이행

* 2.6.6~7 항목은 ZTNA 제품에서 지원

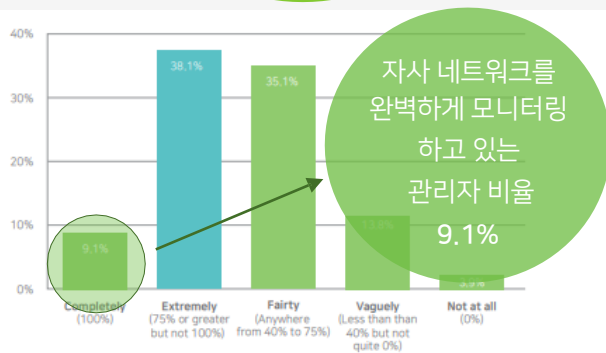
2.10.6 업무용 단말기기 보안 / 2.10.7 보조저장매체 관리

- PC, 모바일, 가상PC, 태블릿 등 사용되는 단말기 기기인증, 승인, 접근범위 설정, 기기보안설정 통제 정책 마련 및 수립•이행
- 외장하드, USB메모리, CD등 보조 저장매체 취급(사용/미사용 제어), 보관 폐기, 재사용에 대한 정책 절차 수립 및 이행

[ISMS 인증기준과 NAC 활용 분야 대비]

Genian NAC의 가시성

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



자사 네트워크를
완벽하게 모니터링
하고 있는
관리자 비율
9.1%

<출처 : SANS BYOD Security Survey>

네트워크 단말의 수량 및 다양성 증가↑

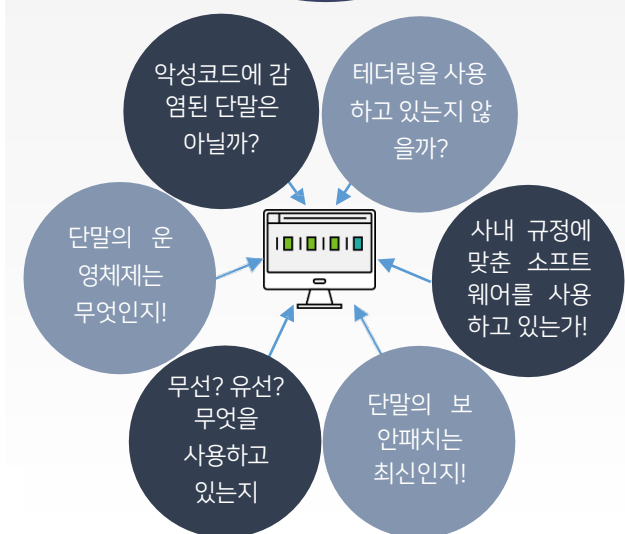


다양한 인사DB 연동(조직도 연동)

IP주소	MAC주소	인증사용자 ↓	플랫폼
172.29.114.94	V6 2C:F0:5D:23:31:84	user1	Microsoft Windows 10 Professional x64
172.29.25.144	V6 A4:5E:60:F1:D3:4B	user2	Apple Device
172.29.59.194	V6 18:C0:4D:DE:7D:50	user3	Microsoft Windows



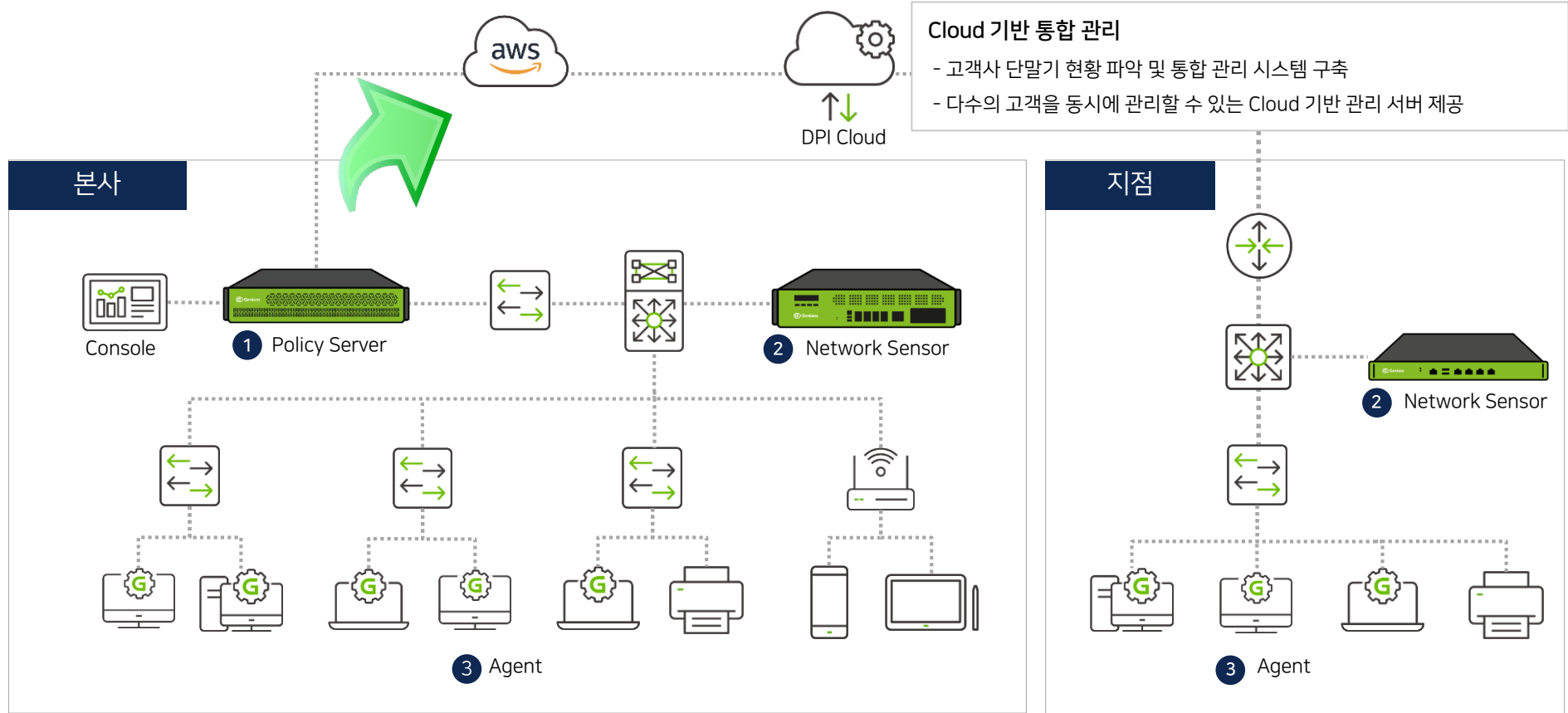
사용자/ 부서별 정책 관리



02.

Genian NAC 제품 소개

NAC 구성



1 Policy Server & Console (정책서버 & 콘솔)

- 유무선 네트워크를 통합 관리하고 내부 보안을 강화할 수 있도록 지원

2 Agent (에이전트)

- PC 등 에이전트 설치 단말에 대한 자산 관리 및 장치사용 통제
- 에이전트 설치에 따른 비용 부담 없음(필요에 따라 선택적 사용)

2 Network Sensor (차단센서)

- 유무선 단말에 대한 정보를 수집하고 강력한 통제 수행
- 포트 별 802.1Q 설정을 통한 효율적인 운영 지원

4 Cloud NAC

- 단말 관리 및 제어 플랫폼을 Cloud 기반으로 제공
- 단말 관리 사업을 위해 필요한 다수의 솔루션을 하나의 솔루션으로 대체 가능
- 단일 관리 콘솔 기반으로 각 기능의 유기적 통합 관리 가능

On-premise NAC vs Cloud NAC



On-premise 방식



제품형 설치

- CC인증서/GS인증서 획득
- Appliance 제품/ 정책서버와 차단센서를
고객사 내부 환경에 설치
- 고객 네트워크 및 보안 정책에 맞춘 시스템 구성 지원
- 정책서버 정책 관리 및 정기 방문 점검 서비스 지원
- 도입 후 1년 무상 유지관리 지원 및
이후 유지관리 계약을 통한 기술지원 지속 제공
- 고객사 전담 엔지니어를 통한 안정적인 시스템 운영 지원

VS



Cloud NAC 방식



Cloud Hybrid 설치

- CSAP 인증서 획득
- 정책 서버는 Cloud에서 운영 (SLA 99.95% 보장)
- 서비스 SLA 보상 기준
 - 99.0% 이상 ~ 99.5% 미만 -> 월 요금 10%
 - 95.0% 이상 ~ 99.0% 미만 -> 월 요금 20%
 - 95% 미만 -> 월 요금 30%
- 초기 구매 비용 낮음
- 가장 최신의 펌웨어 자동 업데이트 관리
 - 신규 기능 적용, 최신 보안 업데이트 제공

가시성 (1/3)

네트워크 내의 모든 단말기 정보 수집 및 분류, IP 실명 확인

장치구분	동작 상태	인증정보	인증시간	IP/MAC		OS/모델 상세 정보	적용받는 제어정책	관리 센서	장비 호스트명	일주일간 동작 차트	장비명/센서명
NT AG ↓ S		인증사용자	최근 사용자인증	IP주소	MAC주소	플랫폼	제어정책	센서명	호스트명(이름)	동작상태차트	장비명 / 센서명
☐		오준혁	2022-05-09 09:08:56	172.29.20.7 VE	E0:D5:5E:86:9A:0C	Microsoft Windows 10 Professional x64	기본정책 ①	S-172.29.20.4	DESKTOP-FMF09D3		S-172.29.20.4 / eth1.20
☐		최문규	2022-02-09 08:26:09	172.29.30.207	88:36:6C:F5:55:58	Microsoft Windows 11 Home x64	기본정책 ①	S-172.29.30.4	문규		S-172.29.30.4 / eth1.30
☐		최유신	2022-02-15 13:29:40	172.29.25.76	B4:B6:76:AB:2E:E4	Microsoft Windows 10 Professional x64	예외허용(EDR개발실) ①	S-172.29.25.4	CHOISEOYUN		S-172.29.25.4 / eth0.25
☐		신학선	2022-02-09 08:32:49	172.29.30.142 VE	34:29:8F:73:69:32	Microsoft Windows 11 Home x64	디펜더 미동작 차단 ①	S-172.29.30.4	신학선-SHINHS		S-172.29.30.4 / eth1.30
☐		김슬기	2022-02-24 08:34:48	172.29.20.18	00:E0:4C:62:7A:80	Microsoft Windows 11 Home x64	기본정책 ①	S-172.29.20.4	DESKTOP-8A03PN8		S-172.29.20.4 / eth1.20
☐		신학선	2022-04-11 13:05:52	172.29.25.167	F4:46:37:8C:16:26	Microsoft Windows 11 Home x64	디펜더 미동작 차단 ①	S-172.29.25.4	신학선-SHINHS		S-172.29.25.4 / eth0.25
☐		윤도연	2022-02-23 08:25:05	172.29.20.129	88:36:6C:F8:5F:0D	Microsoft Windows 10 Home x64	기본정책 ①	S-172.29.20.4	DESKTOP-6G957J9		S-172.29.20.4 / eth1.20
☐		유현	2022-02-15 14:37:07	172.29.25.187	00:C2:C6:B7:39:D2	Microsoft Windows 10 Home x64	GPI 미설치 차단 ①	S-172.29.25.4	DESKTOP-4BRJ5H3		S-172.29.25.4 / eth0.25
☐		강한서	2022-02-21 08:28:32	172.29.20.191	00:0A:CD:31:10:90	Microsoft Windows 10 Home x64	예외허용 ①	S-172.29.20.4	DESKTOP-HFQGA7S		S-172.29.20.4 / eth1.20
☐		권혁이	2022-03-14 09:33:34	172.29.25.102	80:32:53:7A:3B:F9	Microsoft Windows 11 Professional x64	기본정책 ①	S-172.29.25.4	DESKTOP-QNUAL93		S-172.29.25.4 / eth0.25
☐		이민상	2021-10-28 15:12:57	172.29.59.33 VE	00:0C:29:33:06:27	Microsoft Windows 7 Professional x64 ⚠	예외허용(EDR개발실) ①	S-172.29.59.4	MSLEE-PC		S-172.29.59.4 / eth0.59
☐		박민중	2022-04-29 11:59:48	172.29.25.33	CC:15:31:F9:29:14	Microsoft Windows 10 Professional x64	기본정책 ①	S-172.29.25.4	DESKTOP-QAQ6T18		S-172.29.25.4 / eth0.25
☐		안훈기	2022-02-16 09:04:49	172.29.20.123 VE	6C:5A:B0:6C:22:36	Microsoft Windows 10 Home x64	기본정책 ①	S-172.29.20.4	Goodrichgil		S-172.29.20.4 / eth1.20
☐		권혁이	2022-02-09 08:08:01	172.29.30.129	00:E0:4C:62:9E:CC	Microsoft Windows 11 Professional x64	기본정책 ①	S-172.29.30.4	DESKTOP-QNUAL93		S-172.29.30.4 / eth1.30
☐		이민상	2021-10-05 17:27:00	172.29.59.32 VE	00:0C:29:39:5A:E1	Microsoft Windows 7 Professional x64 ⚠	예외허용(EDR개발실) ①	S-172.29.59.4	MSLEE-PC		S-172.29.59.4 / eth0.59
☐		이준수	2022-02-24 10:19:37	172.29.25.166	A0:78:17:69:B1:B1	Apple macOS Monterey	기본정책 ①	S-172.29.25.4	leejsui-MacBookPro.local		S-172.29.25.4 / eth0.25

GUI Column	Column Description	Column Sample Value
인증사용자	해당 장비를 사용 중인 인증 사용자 이름	오승환
최근 사용자인증	최근 사용자인증을 한 시각	2022-05-09 09:08:56
IP주소/MAC주소	해당 단말이 사용 중인 IP와 MAC 주소	172.29.20.7 / E0:D5:5E:86:9A:0C
플랫폼	해당 단말의 플랫폼	Microsoft Windows 10 Professional x64
제어정책	해당 단말이 적용 받는 네트워크 정책	기본정책
호스트명	해당 단말의 호스트명	DESKTOP-FMF09D3

PC 내의 다양한 정보 제공

기본정보

장비정보

시스템정보

네트워크정보

소프트웨어정보

운영체제/업데이트 정보

이력관리

IP관리

정책

정책현황

장비명

M30 노트북

장비 ID

39831ce-c2b0

장비설명

전설업 업무를 노트북

장비 수명주기 관리

제조일

2019-01-03

구입일

구매등록서 일괄 구매

내용연수 시작일

2019-03-01

내용연수 종료일

2021-03-01

내용연수 시작일과 내용연수를 설정하면 내용연수 만료일이 자동으로 입력됩니다

일반번호

123456789

구입가격

1,200,000

책임자

김민지

책임부서

구매부

메모

기본정보

장비정보

시스템정보

네트워크정보

소프트웨어정보

운영체제/업데이트 정보

이력관리

IP관리

정책

정책현황

마더보드 정보

마더보드 제조사

CPU 명

CPU 제조사

Micro-Star International Co., Ltd

Intel(R) Core(TM) i7-4720HQ CPU @ 2.60GHz

Intel Corporation

메모리 정보

전체

사용

% 사용

15.92 GB

2.86 GB

18%

자랑장치 정보

장치명

유형

분타번호/모델

고용번호

파일시스템

총 용량

사용량

용량

% 사용

C

고장드라이브

/ Toshiba THNSNJ25608NU

15GB/100VNTMY

NTFS

227.26 GB

209.21 GB

92%

D (리플리크)

고장드라이브

/ LITEON CV1-88128

002543120268

NTFS

119.24 GB

71.01 GB

60%

E (DriveCD)

고장드라이브

/ Toshiba THNSNJ25608NU

15GB/100VNTMY

NTFS

10 GB

9.38 GB

94%

운영체제 정보

운영체제 명

버전

서비스팩

본 번호

언어

사용자

조직

Microsoft Windows 10 Professional x64

10.0.16299

11.399.16299.0

Korean

zzord

설치명

도메인

제품 Key

설치일자

방화벽

가동시간

자동 업데이트

예약작업

활성화스크랩

FOREST-126

WORKGROUP

2017-10-18 11:53:31

사용중

8 일, 22 시, 57 분

사용안함

사용함

허용안함

엔티테이 정보

이름

MAC

지정 이름

팀

이름

한글명

아랍어명

인터넷연결용

순환명

DynamicIP

SSID

FOREST-126

082B0A11-4A4C

기본정보

장비정보

시스템정보

네트워크정보

소프트웨어정보

운영체제/업데이트 정보

이력관리

IP관리

정책

정책현황

트래픽 정보 (프로토콜)

프로토콜

전체

Output

트래픽 정보 (목적지)

목적지주소

전체

Outgoing

Incoming

업데이트시간

알지한 AP 목록

SSID

MAC

암호화방식

상태

신호 강도

채널

등록원시각

프로토콜

동작상태

B645SID

TCP 세션 정보 (방글간 / 최대값)

세션 상태

CLOSED

ESTABLISHED

CLOSE_WAIT

TIME_WAIT

SYN_SENT

알지한 서비스 목록

구분

정보

등록원시각

업데이트시간

동작

SMB 공유

OS: Windows 10 Pro 16299 (Windows 10 Pro 6.3) NetBIOS computer name: FOREST-126 Workgroup: WORKGROUP System time: 2018-

2018-03-23 14:03:42

2018-04-02 08:41:00

알지한 포트 정보

포트

프로토콜

포트

프로세스명

네트워크 서비스

상태

등록원시각

에이전트

TCP

135

SVCHOST.EXE

RPC

동작함

2018-03-29 08:50:44

에이전트

TCP

139

SYSTEM

NetBIOS 세션 서비스

동작함

2018-03-29 08:50:44

에이전트

TCP

445

SYSTEM

SMB

동작함

2018-04-02 08:37:35

에이전트

TCP

4441

INSAFEPCROSSWERKSVCS.EXE

동작함

2018-03-29 08:50:44

에이전트

TCP

5939

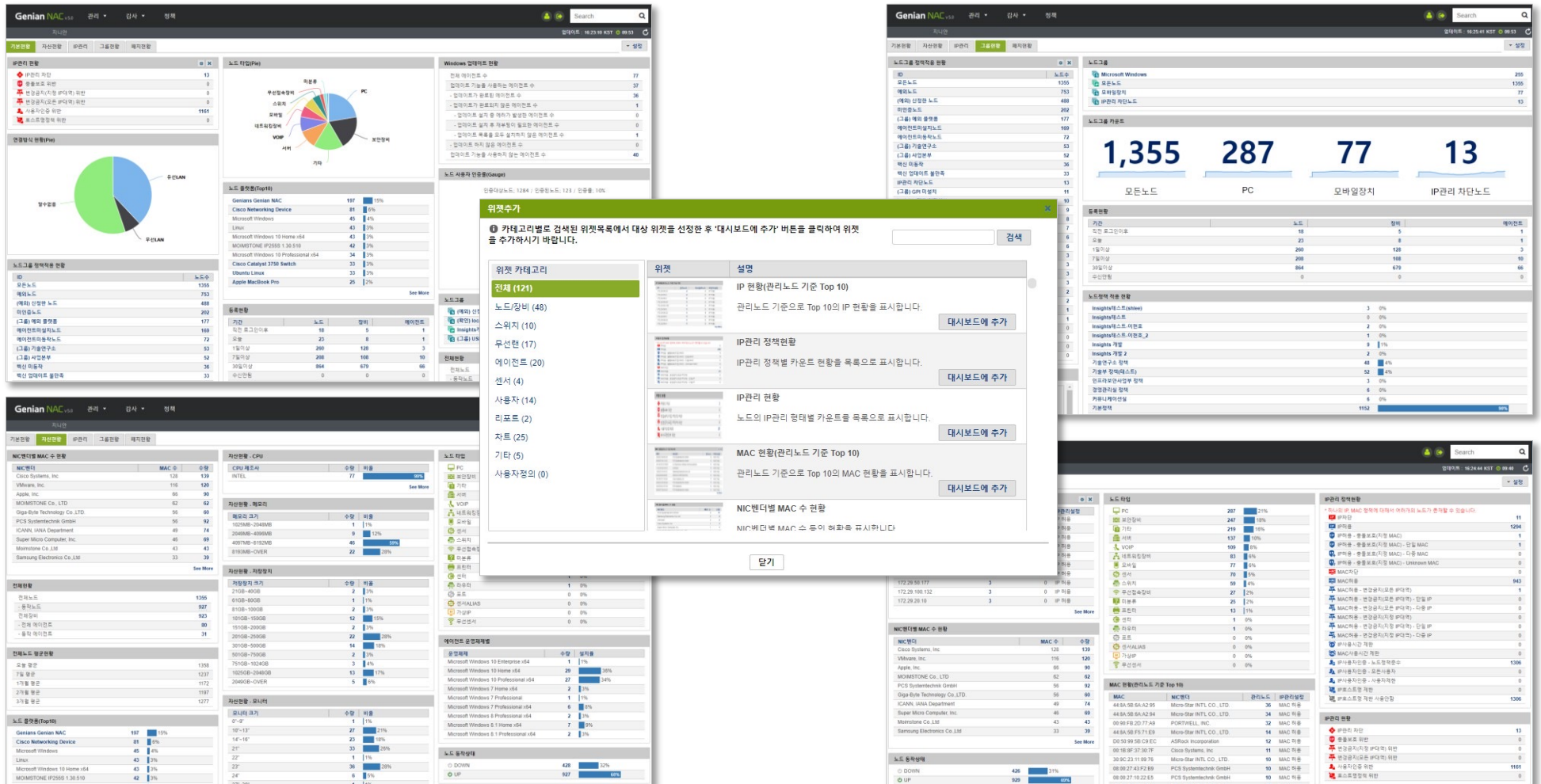
TEAMVIEWER_SERVICE.EXE

동작함

2018-03-29 08:50:44

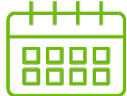
기본정보	장바정보	시스템정보	네트워크정보	소프트웨어정보	운영체제 업데이트 정보	이력관리	IP관리	정책	정책현황				
작성 정보 작성일 Windows Defender	제품 버전 정보 없음	현재버전 버전명 1.263.1913.0	현재버전 날짜 2018-04-02 05:55:37	실시간 종료	소프트웨어 정보 Genian Agent 이전 버전 정보 요청								
소프트웨어 정보 프로그램명 버전 경로 설치일자 종료일자													
Adobe Acrobat Reader DC - Korean 18.011.20038 C:\Program Files (x86)\Adobe\Acrobat Reader DC\ 20180326 2018-03-29 08:50:44													
Adobe Creative Cloud 4.4.1.298 C:\Program Files\Adobe\ 20180326 2018-03-29 08:50:44													
Adobe Premiere Pro CC 2017 11.1.2 C:\Program Files\Adobe\ 20180326 2018-03-29 08:50:44													
Advanced ZIP Password Recovery (remove only) C:\Program Files\Adobe\ 20180326 2018-03-29 08:50:44													
AhnLab Online Security C:\Program Files (x86)\AhnLab\ASP\Common 20180326 2018-03-29 08:50:44													
AhnLab Safe Transaction 1.3.25.1015 C:\Program Files\AhnLab\Safe Transaction 20180326 2018-03-29 08:50:44													
Ahn-SpamFilter 1.1.8.11 1.0.1.11 C:\Program Files\AhnLab\SpamFilter 20180326 2018-03-29 08:50:44													
Apple Software Update 2.2.0.159 C:\Program Files (x86)\Apple Software Update\ 20171011 2018-03-29 08:50:44													
AquaPlayer 1.9.17.0 C:\Users\zzzzz\AppData\Roaming\AquaPlayer\ 20180326 2018-03-29 08:50:44													
BitTorrent 7.10.0.43917 C:\Users\zzzzz\AppData\Roaming\BitTorrent\ 20180326 2018-03-29 08:50:44													
Canon MB2300 series MP Drivers 1.04 C:\Program Files (x86)\Canon\MP Drivers\ 20180326 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													
기본정보	장바정보	시스템정보	네트워크정보	소프트웨어정보	운영체제 업데이트 정보	이력관리	IP관리	정책	정책현황				
작업명은 Windows 업데이트 모음 Default Windows Update (한국말) ① 최근 수동결과 전체													
업데이트명 분류 월/일 업데이트 상태 설치결과상태 업데이트시각													
2018.03.264기반 시스템용 Windows 10 Version 1709의 Adobe Flash Player 보안 업데이트(KB4088785) 보안 업데이트 2018-03-13 완료 미수행 2018-03-29 10:27:08													
2018.03.264기반 시스템용 Windows 10 Version 1709에 대한 수동 업데이트(KB4088776) 보안 업데이트 2018-03-13 완료 미수행 2018-03-29 10:27:08													
Microsoft Word 2013용 보안 업데이트(KB4011659) 32비트 버전 보안 업데이트 2018-03-13 완료 미수행 2018-03-29 10:27:08													
Microsoft Excel 2013용 보안 업데이트(KB4011659) 32비트 버전 보안 업데이트 2018-03-13 완료 미수행 2018-03-29 10:27:08													
Windows 악성 소프트웨어 제거 도구 x64 - 2018.03.13용(KB4089039) 악성 소프트웨어 제거 도구 2018-03-13 완료 미수행 2018-03-29 10:27:08													
Skype for Business 2015용 업데이트(KB4011659) 32비트 버전 응용 소프트웨어 2018-03-06 완료 미수행 2018-03-29 10:27:08													

Dashboard를 통한 다양한 통계, 상태 등의 현황 파악 용이



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	 On/Off	 패스워드

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

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.

IP관리	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
MAC 차단	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%
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%

제어정책 적용 현황

HDH_netctrl_test	0	0%
예외허용	1012	77%
다중다중 자동 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

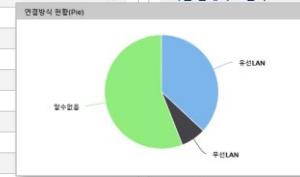
기간	노드	장비	에이전트
직전 로그인 이후	22	2	1
오늘	51	11	2
1일 이상	157	43	4
7일 이상	328	197	10
30일 이상	845	684	64
수신안함	0	0	0

노드그룹 정책적용 현황

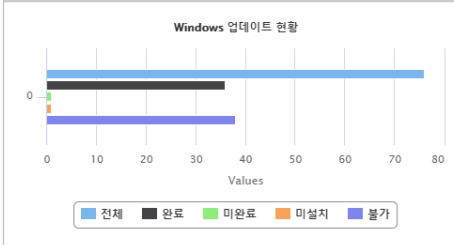
ID	노드수
모든노드	1381
예외노드	725
(예외) 신청한 노드	455
미인증노드	205
에이전트미설치노드	169
(그룹) 예외 플랫폼	162
에이전트미동작노드	57
(그룹) 기술연구소	49
(그룹) 사업본부	48
백신 미동작	40
백신 업데이트 불만족	37
IP관리 차단노드	10
Insights개발(이민상1)	
(그룹) GPI 미설치	
백신 실시간검사 미사용	
패치상태불만족노드	
(예외) 임시 예외노드	
Defender 모니터링 그룹	
PC	
(그룹) 경영관리실	
(그룹) 커뮤니케이션실	5
백신 미존재	4
(그룹) 신규사업TFT	3
Insights테스트(shilee)	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
	8
	7
	7
	7
	6
net51_test	4
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%
에이전트 설치예외	7	1%
임시예외	1	0%
장치제어예외	1	0%
중위험	1	0%

다양한 제어 및 단계적 검증을 통한 보안 강화



알림(Alarm)



차단(Block)



교정(Remediation)

- 사용자에게 알림
(차단 웹, 에이전트 팝업, 인스턴스 메시지)
- 관리자에게 알림
(특정 이벤트 발생 시 SMS, E-mail 발송)
- 특정 로그 외부 전송
(타 보안 솔루션으로 로그 전송하여 모니터링)

- 조건에 따른 네트워크 차단
(신규 IP/MAC, 미 인증, 보안 설정 위반 등)
- 특정 프로세스 중지 (관리자가 지정한 프로세스)
- USB 장치 차단
(USB 저장 장치 등 강제 Off)

- 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, 화면보호기 등)

리포트 (1/2)

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

The screenshot displays the Genian NAC v5.0 interface. The top navigation bar includes '관리' (Management), '감사' (Audit), '정책' (Policy), '설정' (Settings), and '시스템' (System). The '감사' (Audit) tab is active, showing a '로그' (Log) section with a search bar and a '로그검색' (Log Search) section. The '로그검색' section includes a date range selector (1주 | 시작일: 2018-03-26 00:00:00 | 종료일: 2018-04-02 23:59:59) and a chart showing log counts over time. The chart has a legend with categories: ERROR (red), THREAT (orange), WARN (yellow), and INFO (green). Below the chart is a table with columns: 시간 (Time), 로그종류 (Log Type), 로그ID (Log ID), 관리장비명 (Managed Device Name), IP, MAC, 사용자ID (User ID), 사용자명 (User Name), 부서명 (Department Name), and 설명 (Description). The table lists various log entries, including alerts, reports, and system management actions. On the right side of the interface, there are three panels: 'Boolean Operators' explaining logical operators (AND, OR, NOT, etc.), 'Fuzzy Searches' explaining fuzzy search functionality, and a 'Message Template' section for configuring alerts and reports. The 'Message Template' section includes checkboxes for '알람전송' (Alert Transfer), 'SYSLOG 전송' (SYSLOG Transfer), 'SNMP Trap 전송' (SNMP Trap Transfer), and 'Webhook', each with a description of the action. There is also a '태그' (Tag) dropdown menu.

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.

Fuzzy Searches

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

*** 메시지내에 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.

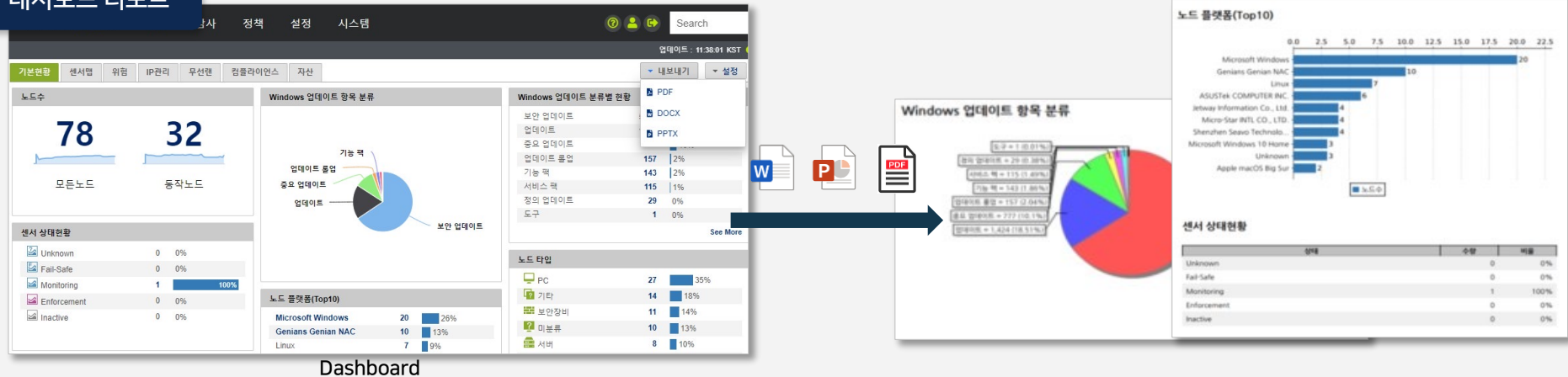
Webhook ☐ 해당 로그 발생시 설정한 URL페이지를 호출합니다.

태그

리포트 (2/2)

대시보드, 노드, 쿼리, 로그 Report 제공

대시보드 리포트



Dashboard

쿼리 리포트

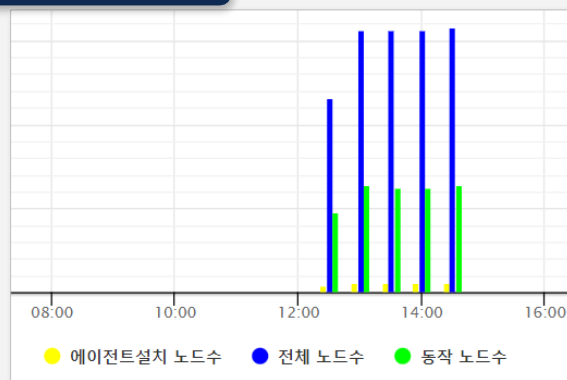
출력파일 (Output File): EXCEL(xls) (Report data will be exported in this format.)

메일수신 (Email Reception): On (Whether to receive email for generated reports.)

수행쿼리 (Executing Query): SELECT * FROM NODE

※ 쿼리를 통해 추출한 데이터를 Excel형태로 제공
 ※ 설정한 주기에 따라 관리자에게 E-Mail 송신

노드 리포트



※ 설정한 데이터의 기간 별 평균, 최대값 통계 제공

로그 리포트

이름	오늘	전일	전주	전월	전일비	전주비	전월비
에러	8	12	12	0	-4	-4	8
위험	0	0	0	2	0	0	-2
경고	0	0	0	201	0	0	-201

※ 로그 별 발생 추이 통계 제공

기능 요약

Agent-less

※ Agent 없는 환경에서도 다양한 방식으로 접근제어

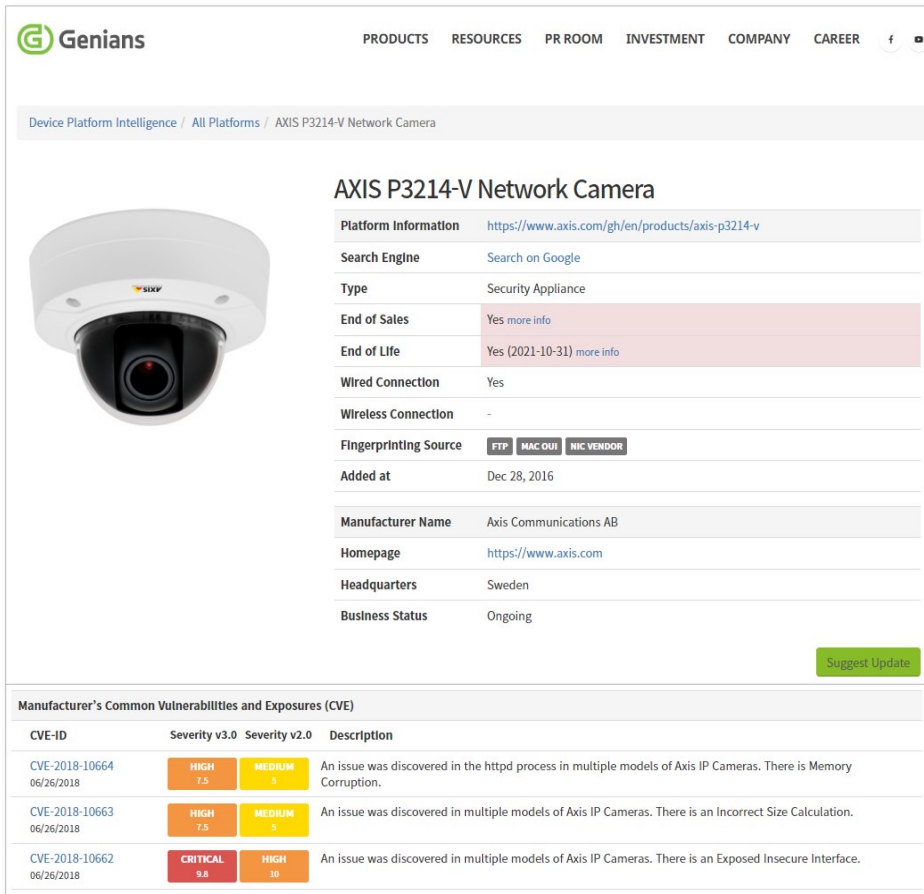
Platform 분류	OS(Windows, Linux, Unix, iOS, Android 등), 네트워크 장비, 프린터, 제조사 등
접근제어	IP, MAC, PORT, Protocol 별 접근 제어
	Platform 별 접근 제어(OS 및 장치 별)
	시간/요일/기간 접근 제어
	사용자 별 접근 제어 (인증/미 인증, ID, 부서, 직급 등)
네트워크 정보	IP 관리 (IP/MAC 고정, 변경금지, 충돌보호, 사용시간 등)
	사용자 PC 가 연결된 스위치 및 포트 정보
	Host 명, Domain 명
	PC 동작 유무 판단, PC 열린 포트 정보

Agent

Windows 패치	Windows patch(PMS) 기능 제공	
세션제어	TCP 세션 정보 수집 및 임계치 초과 시 차단	
포트 정보	열린 포트, 포트 사용 프로세스, 서비스 정보	
장치 제어	USB, NIC, Bluetooth, Wifi, Tethering, PC전원 제어	
프로세스 제어	특정 프로세스 강제 종료	  
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)	
보안 기능	윈도우 보안 설정, 자동 실행 제어, 무선랜 제어, 호스트명 변경, 화면보호기 제어, 파일배포, 계정 취약성 검사	 
위 번조 탐지	IP, MAC clone 탐지/차단	
AP 탐지	무선 AP 탐지 및 접속 제어	 
시스템정보	PC OS 및 H/W 정보(CPU, MEM, DISK, NIC 등), Hostname 수집 및 제어	  
OS 업데이트	OS 자동 업데이트 기능 제공	 
장치 제어	USB, NIC, Bluetooth, Wifi, Tethering	
보안기능	화면보호기 제어, 에이전트 인증, 공유 폴더 제어, 비밀번호 유효성 검사, 파일배포, 방화벽 제어	  

단말 플랫폼 인텔리전스 (Device Platform Intelligence)

DPI를 이용한 단말 제조사 및 취약점 정보확인



AXIS P3214-V Network Camera

Platform Information	https://www.axis.com/gh/en/products/axis-p3214-v
Search Engine	Search on Google
Type	Security Appliance
End of Sales	Yes more info
End of Life	Yes (2021-10-31) more info
Wired Connection	Yes
Wireless Connection	-
Fingerprinting Source	FTP MAC OUI NIC VENDOR
Added at	Dec 28, 2016
Manufacturer Name	Axis Communications AB
Homepage	https://www.axis.com
Headquarters	Sweden
Business Status	Ongoing

[Suggest Update](#)

Manufacturer's Common Vulnerabilities and Exposures (CVE)

CVE-ID	Severity v3.0	Severity v2.0	Description
CVE-2018-10664 06/26/2018	HIGH 7.5	MEDIUM 5	An issue was discovered in the httpd process in multiple models of Axis IP Cameras. There is Memory Corruption.
CVE-2018-10663 06/26/2018	HIGH 7.5	MEDIUM 5	An issue was discovered in multiple models of Axis IP Cameras. There is an Incorrect Size Calculation.
CVE-2018-10662 06/26/2018	CRITICAL 9.8	HIGH 10	An issue was discovered in multiple models of Axis IP Cameras. There is an Exposed Insecure Interface.

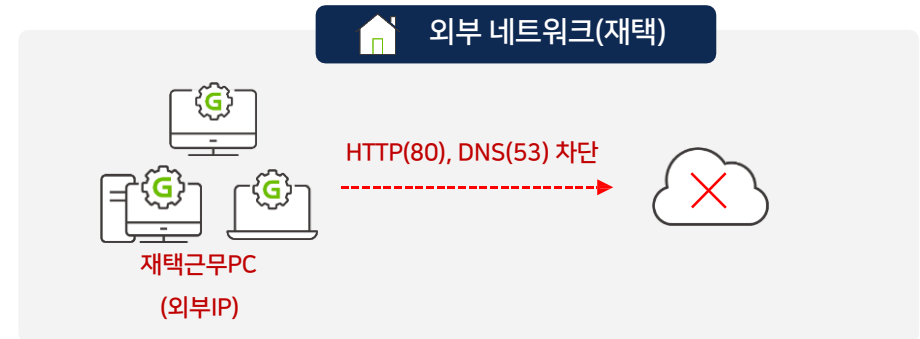
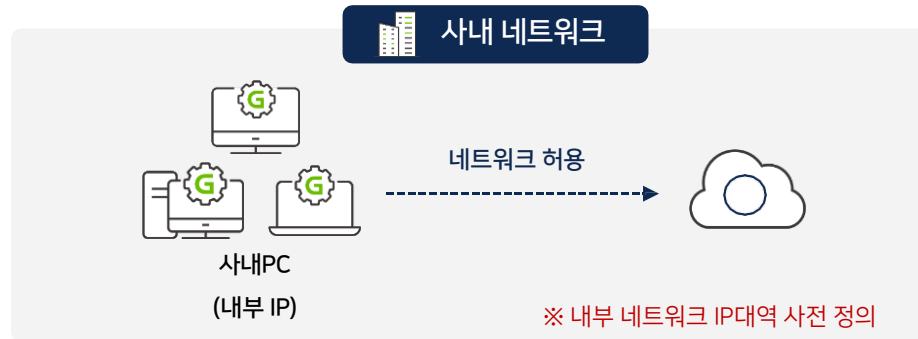
DPI가 제공하는 단말 관련 정보

구분	세부정보
단말 식별 정보 (Device Identity)	· 단말 제조사, 이름, 모델번호 · 단말 사진 · 네트워크 연결 방식(Wired/Wireless) · 단말 상세 정보 URL
단말 확장 정보 (Device Context)	· 제조사 명칭 · 제조사 홈페이지 URL · 본사의 위치와 현재 사업 진행 여부 · 제품 판매 종료(End of Sales) 여부 · 제품 지원 종료(End of Support) 여부 · 검색엔진 연결 URL
단말 위협 정보 (Device Risk)	· 단말에 알려진 CVE 정보 (CVE No. / Severity / Description 등) · 제조사에 알려진 CVE 정보 (CVE No. / Severity / Description 등)

SAML (G-Suite, okta 인증 연동)



업무용 PC 외부 사용 제어



아웃바운드 규칙

이름	그룹	프로필	사용	작업	다시 정의
✓ nProtect Online Security Updater		모두	예	허용	아니오
✓ Wizvera-Delfino-G3-out		모두	예	허용	아니오
✓ Wizvera-Veraport-G3-out		모두	예	허용	아니오
✓ @({Microsoft.BingWeather_4.46.23383.0...}	@({Microsoft.BingWeather_...	모두	예	허용	아니오
✓ @({Microsoft.DesktopAppInstaller_1.4.31...}	@({Microsoft.DesktopAppIn...	모두	예	허용	아니오
✓ @({Microsoft.GetHelp_10.2011.33361.0_...	@({Microsoft.GetHelp_10.20...	모두	예	허용	아니오
✓ @({Microsoft.Getstarted_9.13.33161.0_x...	@({Microsoft.Getstarted_9.1...	모두	예	허용	아니오
✓ @({Microsoft.Messaging_4.1901.10241...}	@({Microsoft.Messaging_4.1...	모두	예	허용	아니오
✓ @({Microsoft.Microsoft3DViewer_7.2010...}	@({Microsoft.Microsoft3DVI...	모두	예	허용	아니오
✓ @({Microsoft.MicrosoftEdge_44.18362.4...}	@({Microsoft.MicrosoftEdge...	모두	예	허용	아니오
✓ @({Microsoft.MicrosoftStickyNotes_3.8.8...}	@({Microsoft.MicrosoftStick...	모두	예	허용	아니오
✓ @({Microsoft.MixedReality.Portal_2000.2...}	@({Microsoft.MixedReality.P...	모두	예	허용	아니오
✓ @({Microsoft.MSPaint_6.2009.30067.0_x...}	@({Microsoft.MSPaint_6.20...	모두	예	허용	아니오
✓ @({Microsoft.OneConnect_5.2011.3081...}	@({Microsoft.OneConnect_5...	모두	예	허용	아니오
✓ @({Microsoft.People_10.1909.12456.0_x...}	@({Microsoft.People_10.190...	모두	예	허용	아니오
✓ @({Microsoft.PPIProjection_10.0.18362...}	@({Microsoft.PPIProjection_...	모두	예	허용	아니오
✓ @({Microsoft.StorePurchaseApp_12011...}	@({Microsoft.StorePurchase...	모두	예	허용	아니오



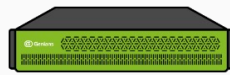
아웃바운드 규칙

이름	그룹	프로필	사용	작업	다시 정의
✗ TCP/80 차단		모두	예	거부	아니오
✗ UDP/53 차단		모두	예	거부	아니오
✓ nProtect Online Security Updater		모두	예	허용	아니오
✓ Wizvera-Delfino-G3-out		모두	예	허용	아니오
✓ Wizvera-Veraport-G3-out		모두	예	허용	아니오
✓ @({Microsoft.BingWeather_4.46.23383.0...}	@({Microsoft.BingWeather_...	모두	예	허용	아니오
✓ @({Microsoft.DesktopAppInstaller_1.4.31...}	@({Microsoft.DesktopAppIn...	모두	예	허용	아니오
✓ @({Microsoft.GetHelp_10.2011.33361.0_...	@({Microsoft.GetHelp_10.20...	모두	예	허용	아니오
✓ @({Microsoft.Getstarted_9.13.33161.0_x...	@({Microsoft.Getstarted_9.1...	모두	예	허용	아니오
✓ @({Microsoft.Messaging_4.1901.10241...}	@({Microsoft.Messaging_4.1...	모두	예	허용	아니오
✓ @({Microsoft.Microsoft3DViewer_7.2010...}	@({Microsoft.Microsoft3DVI...	모두	예	허용	아니오
✓ @({Microsoft.MicrosoftEdge_44.18362.4...}	@({Microsoft.MicrosoftEdge...	모두	예	허용	아니오
✓ @({Microsoft.MicrosoftStickyNotes_3.8.8...}	@({Microsoft.MicrosoftStick...	모두	예	허용	아니오
✓ @({Microsoft.MixedReality.Portal_2000.2...}	@({Microsoft.MixedReality.P...	모두	예	허용	아니오
✓ @({Microsoft.MSPaint_6.2009.30067.0_x...}	@({Microsoft.MSPaint_6.20...	모두	예	허용	아니오
✓ @({Microsoft.OneConnect_5.2011.3081...}	@({Microsoft.OneConnect_5...	모두	예	허용	아니오
✓ @({Microsoft.People_10.1909.12456.0_x...}	@({Microsoft.People_10.190...	모두	예	허용	아니오

※ Windows Defender 방화벽 제어를 통한 외부 네트워크 사용 시 관리자가 설정한 커스텀 규칙 적용

외부 DB서버와 연동을 통한 가시성 확보

DB 연동 지원 범위



NAC
Policy Server

ORACLE
MYSQL
MSSQL/Sybase
IBM DB2
Tibero
Altibase
PostgreSQL
LDAP
CSV
CSV(Upload)
CUBRID
Google G Suite
REST API Server



연동을 통한 가시성 확보



인사 DB

사용자정보

부서정보

직급정보

장비수명주기정보

노드정보



자산관리서버

NT	AG	SS	동작	IP주소	MAC주소	접속포트 ↓	플랫폼
				172.29.100.49	00 90 FB 2D 77 A9	Gi1/0/8	Linux
				172.29.100.150	00 25 90 A0 A2 50	Gi1/0/3	Genians Genian NAC
				172.29.100.200	00 D8 61 56 52 B5	Gi1/0/24	VMware ESXi Server
				172.29.100.217	68 ED A4 25 A6 B0	Gi1/0/16	Genians Genian NAC
				172.29.100.216	68 ED A4 25 A8 D0	Gi1/0/15	Genians Genian NAC
				172.29.100.201	00 D8 61 56 52 89	Fa0/23	Linux
				172.29.100.254	5C A6 2D 04 72 51	Fa0/23	Cisco Networking Device
				172.29.100.60	8C 89 A5 DE 21 07	Fa0/2	VMware ESXi 6 Server
				172.29.100.87	AC 1F 6B 45 2E 58	Fa0/19	Genians Genian Insights Security Appliance
				172.29.100.100	AC 1F 6B 4A 82 16	Fa0/19	Supermicro Intelligent Management IPMI

추가 정보

추가 정보

추가 정보

추가 정보

기존에 운영 중인 시스템의 데이터를 연동하여 추가적인 가시성 확보

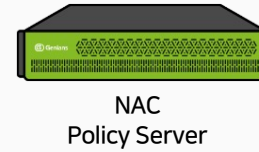
제품 특징점

장비 수명주기 관리

연동을 통한 가시성 확보



장비정보전송



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



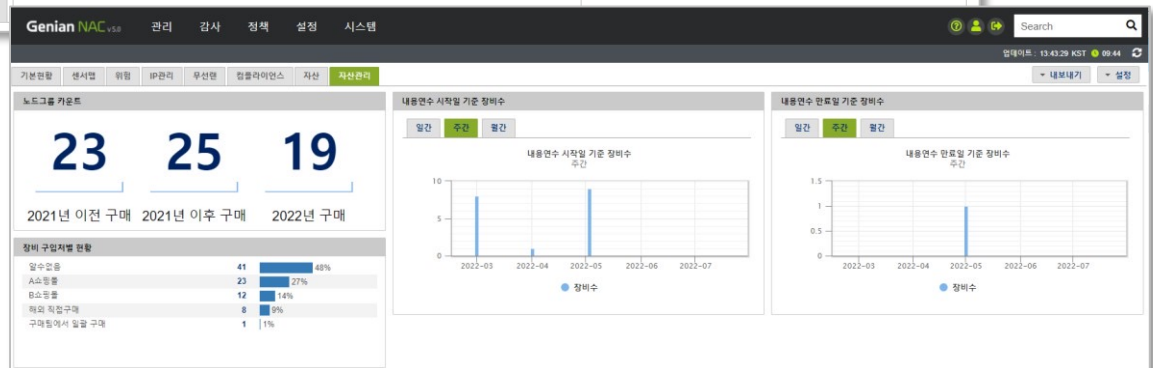
장비정보

장비명	a01-노트북	장비 ID	472ce004-4a76-103c-8001-00e04cac69cd
장비설명	컨설팅 업무용 노트북		

장비 수명주기 관리

제조일	2022-05-01	구입처	구매팀에서 일괄 구매
내용연수 시작일	2021-05-01	내용연수	1 개월
일련번호	123456789	내용연수 만료일	2025-05-01
책임자	김관리	구입가격	1200000
		책임부서	구매부
메모			

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

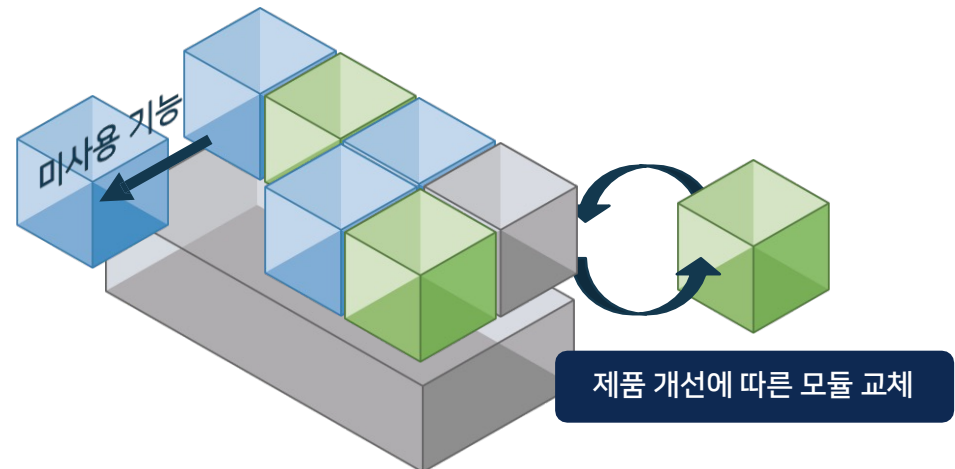


사용자 PC의 안정성을 보장하는 Agent

OS	PT	RA	액션명	플러그인명
Windows	SG	Shield	ARP 관리	ARP 관리
Windows	SG	Shield	DNS 제어	DNS 제어
Windows	SG	Shield	IE보안옵션 제어	웹브라우저 옵션 제어
Windows	SG	Shield	Malware Detector	Malware Detector
Windows	SG	Shield	TCP세션검사	TCP세션검사
Windows	SG	Shield	Windows 방화벽 제어	Windows 방화벽 제어
Windows	SG	Shield	Windows 보안설정	Windows 보안설정
Windows	SG	Shield	Windows 업데이트	Windows 업데이트
Windows	SG	Shield	WMI정보수집	WMI정보수집
Windows	SG	Shield	공유프로그램 미존재	수행조건만 검사
Windows	SG	Shield	네트워크 공유폴더	네트워크 공유폴더
Windows	SG	Shield	네트워크 트래픽 제어	네트워크 트래픽 제어
Windows	SG	Shield	네트워크정보 수집	네트워크정보 수집
Windows	SG	Shield	메신저프로그램 미존재	수행조건만 검사
Windows	SG	Shield	모니터정보 수집	모니터정보 수집
Windows	SG	Shield	모양 및 개인설정	모양 및 개인설정
Windows	SG	Shield	무선 연결 관리자	무선 연결 관리자
Windows	SG	Shield	무선랜제어	무선랜제어
Windows	SG	Shield	무선랜제어(외부)	무선랜제어
Windows	SG	Shield	백신정보 수집	백신정보 수집
Windows	SG	Shield	백신프로그램 존재	수행조건만 검사
Windows	SG	Shield	비밀번호유효성검사	비밀번호유효성검사

- 모든 기능 플러그인 형태로 제공하여 선택/추가 용이함
- 선택적 기능 사용으로 리소스 사용 최소화
- Non-Kernel 기반의 동작(OS 충돌 위험 최소화)
- 1,300곳 이상의 고객사에서 검증된 안정성 (최소 150만 대 이상)

Genian NAC Agent



제품 특징점

macOS / Linux Agent

PT	액션명	플러그인명	설명
	운영체제정보 수집	운영체제정보 수집	macOS 운영체제 정보 및 사용자 정보를 수집하여 노드 정보에 반영합니다.
	하드웨어정보 수집	하드웨어정보 수집	마더보드 정보, 메모리 정보, 저장장치 정보를 수집하여 노드 정보에 반영합니다.
	소프트웨어정보 수집	소프트웨어정보 수집	설치된 소프트웨어 목록을 수집하여 노드 정보에 반영합니다.
	네트워크정보 수집	네트워크정보 수집	네트워크 인터페이스 정보를 수집하여 노드 정보에 반영합니다.
	백신정보 수집	백신정보 수집	PC에 설치된 백신 프로그램을 수집하여 노드 정보에 반영합니다.
	macOS 업데이트	macOS 업데이트	macOS의 최신 업데이트 정보를 수집하여 노드 정보에 반영합니다.

macOS 수집 정보

- ☒ Apple OS X Mavericks
- ☒ Apple OS X Yosemite
- ☒ Apple macOS Sierra
- ☒ Apple macOS Mojave
- ☒ Apple macOS Catalina
- ☒ Apple macOS Big Sur

OS	PT	RA	액션명	플러그인명	설명
			ZTNA 연결 관리자	ZTNA 연결 관리자	ZTNA 연결관리자에 대한 옵션 및 동작을 설정합니다.
			네트워크정보 수집	네트워크정보 수집	네트워크 인터페이스 정보와 탐지된 포트 정보를 수집하여 노드 정보에 반영합니다.
			리눅스 업데이트	리눅스 업데이트	Linux의 업데이트 상태를 검사하고 설정에 따른 최신 업데이트를 수행합니다.
			명령어 수행	명령어 수행	명령어 실행 결과를 수집하여 노드 정보에 반영합니다.
			소프트웨어정보 수집	소프트웨어정보 수집	설치된 소프트웨어 목록을 수집하여 노드 정보에 반영합니다.
			운영체제정보 수집	운영체제정보 수집	운영체제 정보를 수집하여 노드 정보에 반영합니다.
			인터페이스 제어	인터페이스 제어	네트워크 인터페이스를 제어합니다.
			하드웨어정보 수집	하드웨어정보 수집	하드웨어 정보를 수집하여 노드 정보에 반영합니다.

Linux 수집 정보

- ☒ Linux
- ☒ Ubuntu 14
- ☒ Ubuntu 15
- ☒ Ubuntu 16
- ☒ Ubuntu 17
- ☒ Ubuntu 18
- ☒ Ubuntu 19
- ☒ Ubuntu 20
- ☒ Ubuntu 21
- ☒ Gooroom 2
- ☒ HamoniKR 3
- ☒ HamoniKR 4
- ☒ TmaxGooroom 2

USB 장치 정보 자동수집 및 조건 설정 그룹 생성

노드정보	장비정보	시스템정보	네트워크정보	소프트웨어정보	운영체제 업데이트 정보	정책	정책현황	Malware	이력관리
수집된 USB 정보 확인									
USB 정보									
클래스명	장치명	제조사	모델명	시리얼	상태				
Bluetooth	AirPods Pro YA - Find My				사용				
Bluetooth	Microsoft Sculpt Touch Mouse				사용				
Bluetooth	iPhone				사용				
기타 장치	Wireless iAP				사용				
Bluetooth	서비스 검색 서비스				사용				
사운드, 비디오 및 게임 컨트롤러	iPhone A2DP SNK				사용				
사운드, 비디오 및 게임 컨트롤러	AirPods Pro YA - Find My Stereo				사용				
Bluetooth	iPhone Avrcp 전송				사용				
Bluetooth	AirPods Pro YA - Find My Avrcp 전송				사용				
Bluetooth	개인 영역 네트워크 NAP 서비스				사용				
Bluetooth	전화 번호부 액세스 PSE 서비스				사용				
기타 장치	MAP MAS-IOS				사용				
Bluetooth	장치 식별 서비스				사용				
기타 장치	GATT				사용				
기타 장치	Wireless iAP v2				사용				
기타 장치	AAP Server				사용				
사운드, 비디오 및 게임 컨트롤러	iPhone Hands-Free HF Audio				사용				
사운드, 비디오 및 게임 컨트롤러	AirPods Pro YA - Find My Hands-Free AG Audio				사용				
Bluetooth	일반 액세스 프로필				사용				
Bluetooth	일반 특성 프로필				사용				

조건설정

항목: USB 장치 정보

조건: 특정 클래스가 존재하면

설정: 특정 클래스가 존재하면

설정메모: [설정내용] 클래스가 존재하면

특정 클래스가 존재하면

특정 클래스가 존재하지 않으면

장치명이 문자열을 포함하면

모델명이 문자열을 포함하면

특정 클래스에 사용중인 장치가 존재하면

특정 클래스에 사용중지된 장치가 존재하면

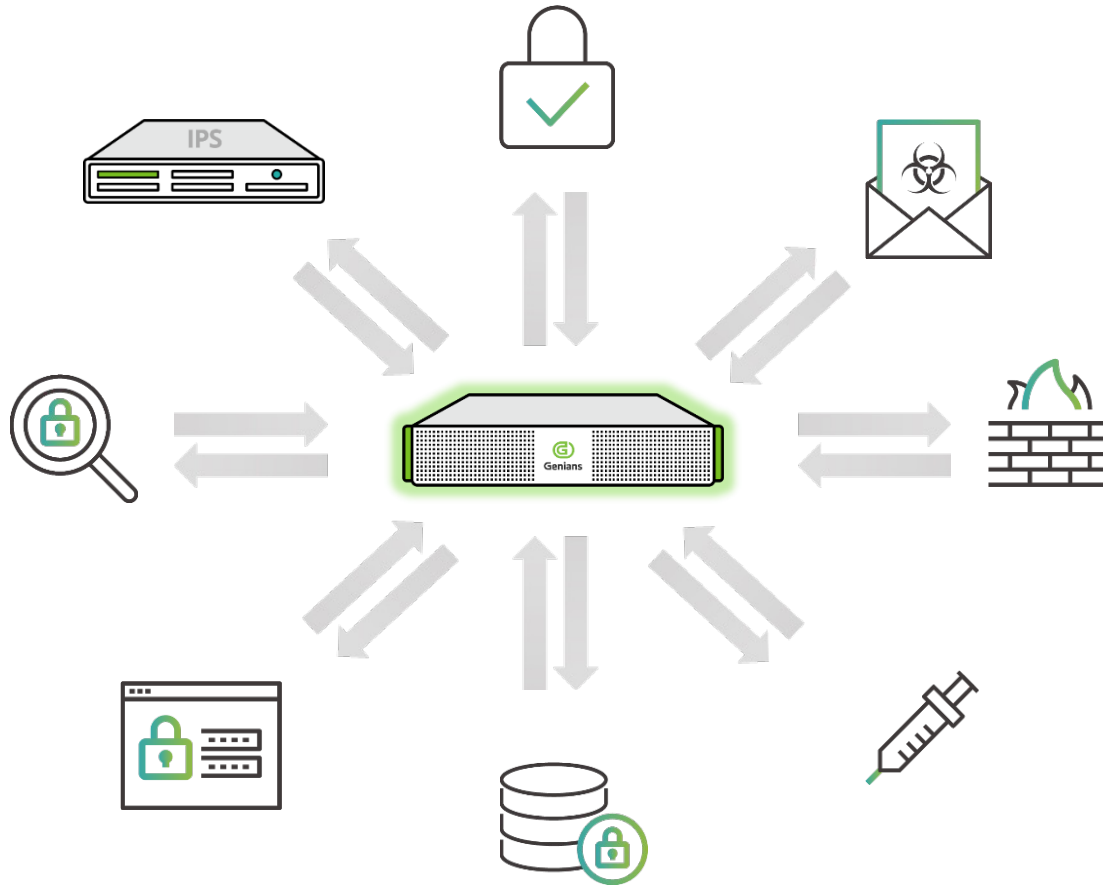
사용중인 장치의 이름이 문자열을 포함하면

사용중이지 않는 장치의 이름이 문자열을 포함하면

다양한조건설정을통해USB장치사용자현황확인

ID	노드수	사용	연산	설정
특정 USB장치 사용자	1	☒	OR	USB 장치 정보 / 특정 클래스가 존재하면 / 카메라 USB 장치 정보 / 장치명이 문자열을 포함하면 / SanDisk
노드그룹: 특정 USB장치 사용자				
NodeGroup = '특정 USB장치 사용자'				
☐ NT AG SS	위험	동작	동작상태차트	IP주소 ↑
☐ 172.30.100.190				MAC주소
				00:E0:4C:68:00:29
				DHCP
				기본정책
				YOONA
				Microsoft Windows 10 Home x64

Security Ecosystem



다양한 보안 시스템과의 연동 제공



Syslog

- 송/수신 기능
- 로그 수신 후 해당 IP 에 대한 제어



Snmptrap

- 송/수신 기능
- 로그 수신 후 해당 IP 에 대한 제어



Rest API

- 타 그룹웨어와의 연동을 위한 유연한 방식
- 신청/결재 시스템 연동



DB 연동

- DB 연동으로 추가적인 정보 제공

가시성 확보와 다양한 형태의 제어, 단계적 검증을 통한 내부 네트워크 보안 강화

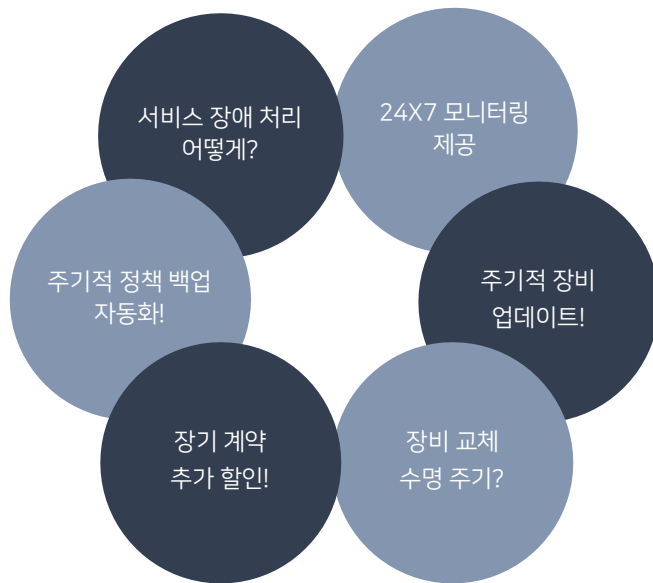
관리의 편리성과 보안 강화

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



제품 특징 비교

Genians Hosted Solution (SaaS)



Genian Cloud NAC (SaaS)



Cloud Hybrid 설치

- 24x7x365 장비 동작 모니터링 수행
- EC2 인스턴스 상태 실시간 모니터링
- 개별 POD 생성 운영
 - EC2 장애 발생시 별도 영역의 EC2로 자동전환
- Managed Service 를 통한 서비스 대응 시간 단축
- 고객 인스턴스 정기적인 백업 (AWS S3 & Glacier)
- 장애 시 자동 복구기능을 통해 서비스 지연 최소화
- 장치 구성간 안전한 암호화 통신 (TLS 1.3)
- 최신 릴리즈 버전 / 펌웨어 상시 업데이트 제공

03.

사용자 스토리

Phase: 가시성 확보 → 비인가단말제어 → 인증 → 무결성검사

2		동작	IP주소 ↑	MAC주소	인증사용자	3	플랫폼	5	접속장치	접속포트	연결방식
NT AG SS	VoIP		172.29.60.19	00:11:A9:6E:7A:40			Moimstone IP255 VOIP Phone		LAB07_DD02	Gi0/16	유선
	PC		172.29.60.31	00:30:48:D6:90:D0			Genians Genian NAC		HP-2920-24G	1	유선
			172.29.60.62	00:E0:4C:68:00:2E			Microsoft Windows		Switch	Gi1/0/1	유선
			172.29.60.63	1C:1B:0D:4C:78:0D			Microsoft Windows 10 Professional x64		LAB07_DD02	Gi0/13	유선
			172.29.60.71	10:6F:3F:39:53:55			Buffalo WHR-HP-G300N Wireless Router		LAB07_DD02	Gi0/13	유선
네트워크 보안장비			172.29.60.73	00:0C:29:74:CE:BB			Genians Genian NAC		Switch	Gi1/0/1	유선
			172.29.60.74	00:0C:29:74:DF:C3			Genians Genian NAC		Switch	Gi1/0/1	유선
			172.29.60.93	D0:27:88:D9:3C:2A			Microsoft Windows Server 2016		LAB08_DD01	Gi0/1	유선
서버			172.29.60.100	D4:5D:64:55:23:0B			Linux		Switch	Gi1/0/1	유선
			172.29.60.106	40:8D:5C:70:7F:05			Microsoft Windows		LAB08_DD01	Gi0/1	유선
			172.29.60.119	70:5D:CC:2E:B0:41			Microsoft Windows		LAB08_DD01	Gi0/1	유선
			172.29.60.120	04:D4:C4:00:06:1F			Microsoft Windows		LAB07_DD02	Gi0/15	유선
			172.29.60.121	FC:AA:14:4C:47:64			Microsoft Windows		LAB07_DD02	Gi0/15	유선
			172.29.60.126	00:0C:29:0D:A6:63			Microsoft Windows Server 2016		Switch	Gi1/0/2	유선
			172.29.60.138	AE:EB:24:A5:6F:29			Unknown		Switch	Fa0/3	유선
			172.29.60.139	68:A8:6D:5E:84:2A			Apple Airport Express AP		LAB07_DD02	Gi0/15	유선
			172.29.60.254	5C:A6:2D:04:72:44			Cisco Networking Device		Switch	Gi1/0/1	유선

순서	설명	
1	차단센서 물리적인 설치 완료	물리적인 장비 설치가 끝나면 네트워크 스캔을 시작하고 수집된 정보를 기반으로 타입과 플랫폼을 분류합니다.
2	각 단말의 종류(PC/ 프린터/ 서버/ 모바일 등) 분류	
3	호스트명/ OS 정보 수집	
4	NAC 사용자 인증 전단계로 사용자 정보는 확인 할 수 없음	
5	스위치 SNMP 연동(SNMP community)을 통해 위치 정보 확인	

Phase: 가시성 확보 → 비인가단말제어 → 인증 → 무결성검사

“보여야 알 수 있고 알아야 관리할 수 있다”



NC250

- ✓ 1분이면 안방까지 뚫린다 ... 사물인터넷 파고든 해킹 (KBS)
- ✓ 안방 CCTV를 누군가 훑쳐본다...스마트 홈 파고드는 'IoT 해킹' (동아일보)
- ✓ IP 카메라 해킹해 남의 집 안방 훑쳐본 외국인 강사 벌금형 (연합뉴스)
- ✓ 홈 IoT 도어락 해킹해 10초만에 딸깍 (보안뉴스)
- ✓ '실종된 사생활'...IoT 해킹경고 (디지털타임스)
- ✓ “현관문 따고 집안 훑쳐보고”...‘IoT 60%’ 스마트홈 해킹 ‘송송’ (KBS)

Platform's Common Vulnerabilities and Exposures (CVE)

CVE-ID	Severity v3.0	Severity v2.0	Description
CVE-2017-10796 07/02/2017	MEDIUM	LOW	On TP-Link NC250 devices with firmware through 1.2.1 build 170515, anyone can view video and audio without authentication via an rtsp://admin@yourip:554/h264_hd.sdp URL.

비인가 사용자가 비디오 파일, 오디오 파일에 접근할 수 있는 취약점

Phase: 가시성 확보 → 비인가단말제어 → 인증 → 무결성검사

2

시스템정보

마더보드 정보

새시 유형	마더보드 제조사	CPU 명	CPU 제조사	리비전	배터리	온도	CPU 사용량
Notebook	SAMSUNG ELECTRONICS CO., LTD.	Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz	Intel Corporation	526058	준재합		37.02%

메모리 정보

메모리 전체	사용	% 사용
8 GB	5 GB	59.70%

저장장치 정보

장치명	유형	벤더명/모델명	고유번호	볼륨ID	파일시스템	총 용량	사용된 용량	% 사용
C:	고정드라이브	/ SAMSUNG MZVLW256HEHP-000	3338_5A30_4B14_7749_0025_3858_0000_0001	ECD6-7A4B	NTFS	223 GB	189 GB	84.99%

운영체제 정보

운영체제 명	버전	빌드 버전	서비스팩	IE 버전	언어	사용자	조직		
Microsoft Windows 10 Home x64	1903	10.0.18362		11.1016.18362.0	Korean	MC			
제품 Key	호스트명	도메인	설치된시각	방화벽	가동시간	자동업데이트	최근패치시각	예약작업	원격데스크톱
YR229-NB77P-JFKKK-JV8VC-P9XQR	MC	WORKGROUP	2019-09-19 12:16	사용중	1 일, 4 시간	자동설치 매일 오전 12:00	2021-03-23 04:27	사용할	허용안함

인터페이스 정보

이름	연결방식	MAC	장치이름	링크
Bluetooth 네트워크 연결	Bluetooth	A0:C5:89:AA:38:99	Bluetooth Device (Personal Area Network)	DOWN
SSTAP 1	유선	00:FF:FD:FA:40:DE	TAP-Windows Adapter V9 #2	DOWN
Wi-Fi	무선	A0:C5:89:AA:38:95	Intel(R) Dual Band Wireless-AC 8265	DOWN
로컬 영역 연결* 1	무선	A0:C5:89:AA:38:96	Microsoft Wi-Fi Direct Virtual Adapter	DOWN
로컬 영역 연결* 4	무선	A2:C5:89:AA:38:95	Microsoft Wi-Fi Direct Virtual Adapter #2	DOWN
이더넷 11	유선	00:E0:81:35:D2:07	Realtek USB FE Family Controller #2	UP

순서

설명

1

설치된 단말의 시스템 정보 수집 사전 배포

2

각 단말의 종류(PC/ 프린터/ 서버/ 모바일 등) 분류
 - 하드웨어 정보: 마더보드/ CPU/ 메모리/ 저장장치/ 인터페이스 등 정보수집
 - 운영체제 정보: 운영체제/버전/빌드 버전/언어 등 정보수집
 - 공유폴더/ 화면보호기/ 윈도우 방화벽/ 호스트명 변경(인사DB 활용)
 - 사용자계정 정보: 비밀번호 규칙(변경주기)/ 계정타입(관리자, 사용자)에 따른 제어

기 운영 중인 배포 시스템이 있다면 NAC Agent 를 사전배포(강제화 전)하여 단말의 가시성을 확보할 수 있습니다.

Phase: 가시성 확보 → 비인가단말제어 → 인증 → 무결성검사

1 소프트웨어목록

프로그램명	버전	경로	설치일자	등록된시간
3D Builder	18.0.1931.0	C:\Program Files\WindowsApps\Microsoft.3DBuilder_18.0.1931.0_x64__8wekyb3d8bbwe		2022-05-12 14:11
3D 뷰어	7.2107.7012.0	C:\Program Files\WindowsApps\Microsoft.Microsoft3DViewer_7.2107.7012.0_x64__8wekyb3d8bbwe		2022-05-12 14:11
Adobe Acrobat Reader DC - Korean	22.001.20117	C:\Program Files (x86)\Adobe\Acrobat Reader DC\	2022-04-15	2022-05-12 14:11
AhnLab Safe Transaction	1.5.1.1581	C:\Program Files\AhnLab\Safe Transaction	2020-08-05	2022-05-12 14:11
Amazon	2018.519.2815.0	C:\Program Files\WindowsApps\Amazon.com.Amazon_2018.519.2815.0_x64__343d40qqv1t		2022-05-12 14:11
AnySign4PC 1.1.3.3	1.1.3.3			2022-05-12 14:11
Apple 응용 프로그램 지원(32비트)	6.4	C:\Program Files (x86)\Common Files\Apple\Apple Application Support\	2018-05-09	2022-05-12 14:11
Apple 응용 프로그램 지원(64비트)	6.4	C:\Program Files\Common Files\Apple\Apple Application Support\	2018-05-09	2022-05-12 14:11
AsyncTextService	10.0.19041.1023	C:\Windows\SystemApps\Microsoft.AsyncTextService_8wekyb3d8bbwe		2022-05-12 14:11
Autodesk SketchBook	5.1.0.0	C:\Program Files\WindowsApps\89006A2E.AutodeskSketchBook_5.1.0.0_x64__f1f1gterx813w		2022-05-12 14:11
Beauty Camera	2.0		2018-10-16	2022-05-12 14:11
Bonjour	3.1.0.1	C:\Program Files (x86)\Bonjour\	2018-05-09	2022-05-12 14:11
BrainPOP ESL	1.3.9.0	C:\Program Files\WindowsApps\BrainPOP.LLC.BrainPOPESL_1.3.9.0_x64__w5m80jg9906m		2022-05-12 14:11
Canon Office Printer Utility	12.7.0.0	C:\Program Files\WindowsApps\34791E63.CanonOfficePrinterUtility_12.7.0.0_x64__6e5tt8cgb93ep		2022-05-12 14:11
CapturePicker	10.0.19041.1023	C:\Windows\SystemApps\Microsoft.Windows.CapturePicker_cw5n1h2zyewy		2022-05-12 14:11
Chrome	101.0.4951.64	C:\Program Files (x86)\Google\Chrome\Application	2022-05-12	2022-05-12 14:11
ColorEngine	4.4		2018-10-16	2022-05-12 14:11
Consulting Mode Touchpad Driver	20.0.0.24			2022-05-12 14:11
CoreAAC Audio Decoder (remove only)				2022-05-12 14:11
Cortana	4.2203.4603.0	C:\Program Files\WindowsApps\Microsoft.549981C3F5F10_4.2203.4603.0_x64__8wekyb3d8bbwe		2022-05-12 14:11

순서	설명	
1	설치된 단말의 소프트웨어 정보 수집 - 백신 정보: 설치된 백신명/ 패턴 버전/ 패턴 날짜/ 실시간감시설정/ 최근검사 - 소프트웨어: 소프트웨어명/ 버전/ 설치경로/ 설치일자 등 - 필수소프트웨어 강제 배포, 비인가 프로그램 삭제, 프로세스 킬 등	사전 배포를 통해 NAC Agent가 설치되면 백신/ 일반 소프트웨어 정보 등을 수집할 수 있습니다. 차후 필수 소프트웨어 배포, 프로세스 킬 등의 정책운 영을 위한 정보가 됩니다.

사용자 영역 (IP 관리시스템)

Phase: 가시성 확보 → 비인가단말제어 → 인증 → 무결성검사

Genians

Korean ▼

내정보: IP=172.30.100.190, MAC=00:E0:4C:68:00:29, PC명=YOONA

- ① 사용하시는 컴퓨터가 IP관리정책을 위반했습니다. IP관리 담당자에게 요청해서 허용된 IP또는 MAC주소인지 확인하여 주세요.
- ② 사용자 인증이 요구됩니다. 아래의 "인증" 버튼을 눌러 사용자인증을 받으시기 바랍니다.

인증 확인 IP사용신청 상태재검사

순서	설명	
1	승인되지 않은 단말이 내부망에 연결	승인되지 않은 비인가 단말을 연결하면 IP사용신청 페이지(전통적인 IP관리)로 전환됩니다.
2	네트워크 사용이 차단되고 웹브라우저 사용시 "비인가" 상태 확인	
3	IP"사용신청" 진행 (IPM)	

사용자 영역 (IP 관리시스템)

Phase: 가시성 확보 → 비인가단말제어 → 인증 → 무결성검사

IPManagement Console

IP신청신청

2

사용자ID: testse

사용자명: testse

부서명: 기술팀

사용위치: <선택하세요>

사용종료: 2022-05-31

신청사유: test

3

SMS문자통보: 01040435549

Email통보: test@genians.com

사용자ID	testse
사용자명	testse
부서명	기술팀

SMS문자통보	01040435549 (전화번호 입력시 '-'는 빼고 입력해주세요.)
Email통보	test@genians.com 신청서 처리에 대해서 통보받을 이메일을 설정합니다.

순서	설명
1	신청자의 계정으로 IP"사용신청" 시스템 로그인
2	신청자 정보 확인 및 작성 - 인사DB 연동을 통해 사용자 지정 시 사용자명/ 부서 등 자동표시
3	IP사용 신청 결과를 SMS/Email로 수신할 수 있도록 통보 방법 작성

신청자는 웹기반으로 신규 단말에 대한 사용신청을 진행할 수 있습니다.
사내 인사DB를 연동하여 신청자의 편의성을 확보할 수 있습니다.

사용자 영역 (IP 관리시스템)

Phase: 가시성 확보 → 비인가단말제어 → 인증 → 무결성검사

Genian NAC v5.0 관리 감사 정책 설정 시스템 ? [User Icon] [Logout Icon] Search

업데이트 : 13:54:22 KST

IP신규/반납 신청서

작업선택 신청자명 사용자명 검색 1 - 5 / 5 50

☐	번호	신청서처리	용도	IP	사용자ID	사용자명	부서명	신청자ID	신청자명	신청일자 ↓
☐	25	승인 거부	임시사용	①	③TEMP	조운아	영업지원팀	③TEMP	조운아	2021-03-30 13:54:00
☐	24	승인 거부	임시사용	①	③TEMP	임상혁	네트워크사업부	③TEMP	임상혁	2021-03-30 13:51:53
☐	23	승인 거부	유동IP사용	①	limgw	임건웅	지니언스(주)	limgw	임건웅	2021-03-30 13:50:42
☐	22	승인 거부	유동IP사용	①	amc1321	안민찬	지니언스(주)	amc1321	안민찬	2021-03-29 16:18:28
☐	11	승인 거부	유동IP사용		hyunjini	조현진	지니언스(주)	hyunjini	조현진	2020-10-23 14:39:37

순서	설명	
1	IP신청이 발생시 관리자는 SMS(혹은 E-Mail)로 신청 발생을 인지	사용자가 IP사용 신청을 하면 관리자는 NAC 관리 콘솔에 접속하여 승인/ 거부 과정을 진행합니다. 신청서가 처리되면 사용자(신청자)에게 알림 메시지가 전송됩니다.
2	관리 WEBUI 에서 IP신청서를 승인/거부	
3	추가 기능 - 주요 장비의 충돌보호, 사용자 PC의 변경 금지 설정 등	

Phase: 가시성 확보 → 비인가단말제어 → 인증 → 무결성검사



순서	설명	
1	IP사용 승인 후 NAC 사용자 인증: IP실명제	기기에 대한 승인 이후 사용자에게 인증을 진행합니다. 내부직원은 연동된 인사DB의 아이디 기반으로 인증을 진행하고 외부 사용자는 "사용자 등록" 을 통해 계정신청 을 요청할 수 있습니다.
2	인증된 사용자 정보는 연동된 문서보안, PC보안 에이전트 등에 인증정보를 전송하여 불필요한 인증과정 제거	
3	추가기능 - 외부직원, 프로젝트팀 등 인사DB에 없는 사용자는 "사용자등록" 진행 - 사용자별 인증 가능한 IP/ MAC, 개수 지정 가능 - 아이디/ 비밀번호 찾기(초기화) 기능: SMS, E-Mail - 인증주기: IP/MAC 변경시, 시간, 부팅시 재인증 등	

Phase: 가시성 확보 → 비인가단말제어 → 인증 → 무결성검사

- 1 누가? 2 언제? 3 어디서? 4 어떤 IP/MAC으로? 5 어떤 장비로? 6 어떤 목적으로? 7 어떤 정책을?

☐ NT AG SS	동작	인증사용자	등록시각	접속포트	IP주소	MAC주소	플랫폼	설명	호스트명(이름)	제어정책
☐		임건웅	2021-01-27 15:22:50	Gi0/24	172.30.20.39	00:E0:81:35:D2:04	Microsoft Windows 10 Home x64	NAC 컨설팅 인원	MC	기본정책 ⓘ

	GUI Column	Sample - GUI Value
1. 누가?	인증 사용자	임건웅
2. 언제?	최근 동작, 최초 사용 시각	2021년 01월 27일 15시 22분 50초
3. 어디서?	스위치, 포트	내부 Switch Gi0/24 번 포트
4. 어떤 IP로?	IP주소 / MAC주소	172.30.20.39 / 00:E0:81:35:D2:04
5. 어떤 장비로?	플랫폼	Windows 10 Home x64 를 이용하는 단말
6. 어떤 목적을?	설명 [관리자가 설정하는 설명 글]	외부에서 컨설팅 목적으로 들어온 인원
7. 어떤 정책을?	네트워크 정책	(Role Base Access Control) 협력업체 [IP별 / 서비스별 / 시간별 정책설정]

IP 관리 시스템에서 제공되는 부분

순서	설명
1	IP 실명제 완료
2	네트워크에 연결된 단말별 사용자 정보 수집 완료

사용자 인증을 통해 "IP실명제"가 완료되었고 확보된 사용자기반의 가시성을 통해 사용자/ 부서별 정책에 활용할 수 있습니다.

Phase: 가시성 확보 → 비인가단말제어 → 인증 → 무결성검사



순서	설명	
1	필수 소프트웨어 설치 강제화	NAC Agent가 설치되면 사용자 단말의 가시성을 확보하고 보안 무결성 항목에 대한 강제화를 수행할 수 있습니다. ※ Windows에서 연동 가능한 백신목록 V3, ViRobot, ALYac (알약 연동 모듈)
2	불법 소프트웨어 설치 시 차단, 불법 프로세스 차단	
3	OS 보안 강제화 - 공유폴더/ 화면보호기/ 윈도우 방화벽/ 호스트명 변경(인사DB 활용) - 사용자계정 정보: 비밀번호 규칙(변경주기)/ 계정타입(관리자, 사용자)에 따른 접근 제어	
4	보안/ 중요/ 업데이트/ 업데이트 롤업 등의 패치	

04.

주요 고객사

KEB 하나은행	우리은행	IBK 기업은행
Standard Chartered	MG새마을금고	신협
좋은일이 생깁니다 경남은행	광주은행	신한지축은행
BS저축은행	홍국생명	현대해상
내일을 위한 금융 한화손해보험	동부화재	신한라이프
수호천사 동양생명	ING	MERITZ 메리츠화재
국민과 함께하는 보험 KB생명	한국교직원공제회 The·K손해보험(주)	금융결제원
MIRAE ASSET 미래에셋생명	우리카드	하나카드
Hyundai Card	비씨카드	현대증권
NH투자증권	KDB대우증권	아주캐피탈

Together.
More Secure.