통합 보안 플랫폼 기업, 지니언스

Genians IPAM

Genians

Table of Contents

01. Genian IPAM 개요

IP 관리

개요

네트워크 단말의 효율적인 관리를 위한 첫 번째 단계는 단말 IP/MAC을 관리하고 정책을 수립해 제어하는 것입니다. 빠르게 발전하는 IT기술의 변화와 BYOD(Bring Your Own Device) 트렌드로 인해 스마트폰, 태블릿 등 모바일 단말 사용이 증가하며 네트워크 관리가 더욱 복잡해지고 있기 때문입니다. 자동화된 IP 관리도구는 이제 네트워크 관리자의 필수 선택 사항으로 고정 IP 환경에서부터 DHCP 환경에 이르기까지 네트워크 단말 IP를 확장성을 고려하여 유연하게 관리할 수 있습니다.

NT AG ↑ SS	동작	IP주소	MAC주소	플랫폼
		172.29.20.40 V6	08:60:6E:F8:23:FE	Linux
		172.29.20.153 V6	00:E0:4C:65:E3:4B	Microsoft Windows
		172.29.20.169	A8:E5:39:64:0F:A4	MOIMSTONE IP255S 1.30.510
		172.29.20.45	00:11:A9:6D:5E:8A	Stonehenge IP255-S 1.30.236
		172.29.20.16 V6	1C:1B:0D:4F:35:34	Microsoft Windows 10 Professional x64
		172.29.20.130	00:11:A9:6F:35:94	Stonehenge IP255-F 1.30.238
		172.29.20.174	00:22:B0:F6:76:61	D-Link DIR-100 Ethernet Broadband Router
		172.29.20.227	00:E0:4C:68:06:84	Microsoft IIS 10.0 Server
		172.29.20.8 V6	E0:D5:5E:59:BA:94	Microsoft Windows
		172.29.20.49	00:90:FB:2D:77:A9	Linux
		172.29.20.24	00:08:88:12:26:BE	Oullim SecureWorks Firewall/VPN
		172.29.20.131	A8:E5:39:5A:48:78	MOIMSTONE IP255S 1.30.510
		172.29.20.254	5C:A6:2D:04:72:56	Cisco Networking Device
		172.29.20.116	00:11:A9:80:36:D8	Moimstone IP255 VOIP Phone
		172.29.20.48	A8:E5:39:4B:37:96	MOIMSTONE IP255S 1.30.510
		172.29.20.115	00:11:A9:6D:5E:8A	Stonehenge IP255-S 1.30.236
		172.29.20.22	00:11:A9:6F:35:94	Stonehenge IP255-F 1.30.238
		172.29.20.24	90:9F:33:98:29:01	EFM Networks AP
		172.29.20.52	C4:12:F5:5B:94:FF	D-link device
		172.29.20.3	84:BA:3B:15:47:6B	Canon iR ADV C3530 Printer

02. Genian IPAM 소개

가시성 (Visibility)

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

어떤 IP/MAC을 통해 | 어떤 장비로 | 누가 | 어디서 | 언제

NT AG SS	동작	IP주소	MAC주소	호스트명	플랫폼	인증사용자	위치	마지막 동작시각
		172.29.25.136 V6	B2:D8:36:26:CF:A6	Junsuk-Note20	Android OS	최		2021-10-12 09:04:57
		172.29.25.160 V6	9E:9A:7E:4A:7F:BF	iPhone12	Apple iPhone 12 Phone	진		
		172.29.25.171 V6	06:D2:D6:BB:7B:FB	iPhone12	Apple iPhone 12 Phone	진		2021-10-12 10:04:52
		172.29.25.59	F8:FF:C2:00:5B:66	MACBOOKPRO...	Apple MacBook Pro	조		
		172.29.25.18	F8:FF:C2:00:5B:66		Debian GNU/Linux	조		
		172.29.25.93 V6	18:47:3D:BA:27:0F	yiho25-Dell	Microsoft Windows 10 Home x64	이		
		172.29.25.14 V6	F4:5C:89:B6:D6:A3	hyunho-mac	Apple Device	이		
		172.29.25.18 V6	A0:78:17:69:B1:B1	leejsuicBookPro	Apple MacBook Pro	이		
		172.29.25.148 V6	3A:55:67:B1:4A:22	ijeyeonuiiPhone	Apple iPhone	이		
		172.29.25.169	F8:28:19:AB:3D:25	DESKTOP-3JT1...	Microsoft Windows 10 Home x64	이		
		172.29.25.156 V6	E6:FE:8E:C6:32:D2	ijaeuguiiPhone	Apple iPhone	이		2021-10-12 10:10:54
		172.29.25.133 V6	38:F9:D3:B4:50:35	MACBOOKPRO...	Apple MacBook Pro	이		
		172.29.25.155 V6	80:32:53:B3:90:7A	DESKTOP-SOQ...	Microsoft Windows 10 Professional x64	이		
		172.29.25.110 V6	50:ED:3C:12:EA:B7	MACBOOKAIR-...	Apple MacBook Air	유		
		172.29.25.143 V6	BA:3F:6D:31:F7:EC	dosig-ui-Galaxy-...	Samsung Galaxy Note20 Ultra 5G Phone	신		2021-10-12 09:20:58
		172.29.25.158 V6	32:E0:A0:9B:C8:47	dosig-ui-Galaxy-...	Samsung Galaxy Note20 Ultra 5G Phone	신		2021-10-12 09:35:18
		172.29.251.51	FC:B3:BC:78:13:5B	LAPTOP-8M9R...	Microsoft Windows 10 Home x64	박		
		172.29.25.146 V6	8C:85:90:42:2A:7B	MACBOOKPRO...	Apple MacBook Pro	박		
		172.29.25.101 V6	F8:FF:C2:00:AF:0A	MACBOOKPRO...	Apple MacBook Pro	박		
		172.29.25.99 V6	A6:0F:4D:55:D3:4C	bagminuuiiPhone	Apple iPhone	박		
		172.29.25.98 V6	0A:52:39:2B:E4:8F	bagminunguiiPad	Apple iPad	박		

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) 재 배포(DB Update)
4) 새로운 단말 인식 및 분류

- **장치분류 DB**

PC, Server, Printer, Switch, 보안장비, 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

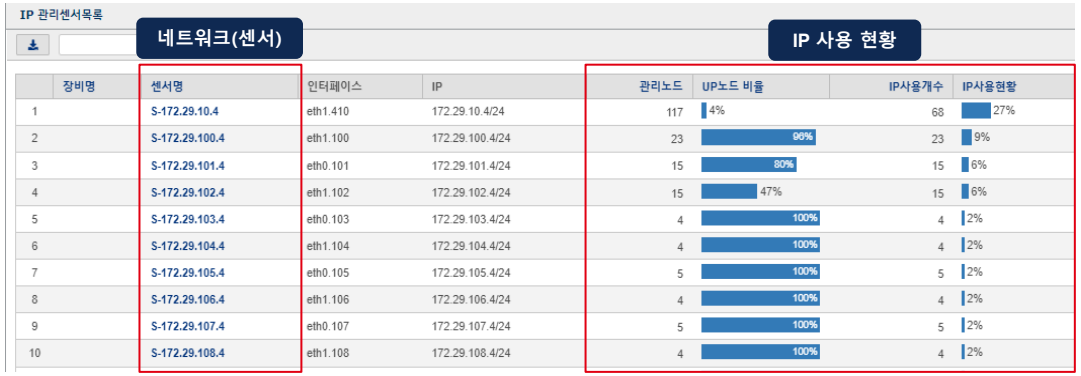
위험	IP	동작	IP주소	MAC주소	정책	호스트명	플랫폼	인증	위치	스위치포트	연결방식
위험 행위 노드	IP정책 위반 노드	UP/Down	IP주소	MAC주소	적용되어 있는 정책	PC이름	종류 / 기기 명칭	**인증된 사용자 ID**	현재 노드가 탐지된 위치	SNMP연동	Agent 및 AP 탐지

가시성 (Visibility)

Matrix View를 통한 IP 사용 현황 파악

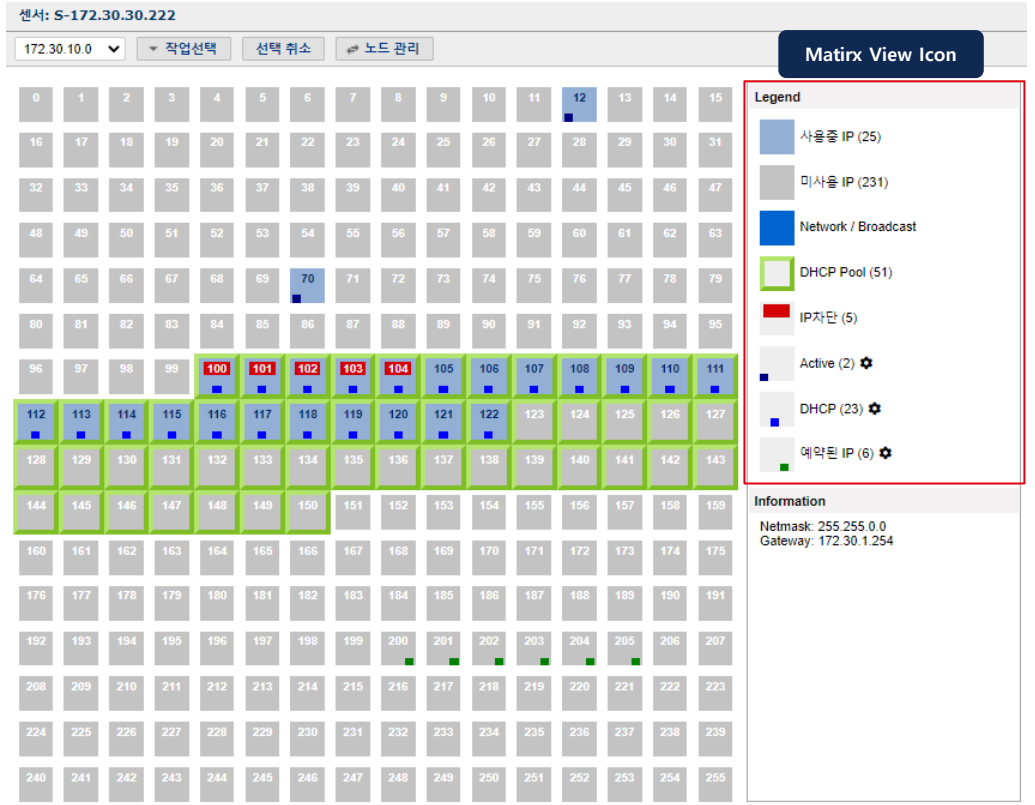
Matrix View 화면을 통해 사용/미사용 중인 IP 현황을 가시성 있게 표현하여, 관리자가 네트워크 별 IP 사용 현황에 대해 한눈에 파악하기 용이하도록 함

- **네트워크 별 IP사용 현황 화면 제공**
  - 네트워크(센서) 별 IP사용 현황, UP 노드 비율 등의 상태 제공
- **IP Matrix View 제공**
  - DHCP IP할당, 사용/미사용 IP 및 정책 현황 정보를 가시성 있게 제공



	장비명	센서명	인터페이스	IP	관리노드	UP노드 비율	IP사용개수	IP사용현황
1		S-172.29.10.4	eth1.410	172.29.10.4/24	117	4%	68	27%
2		S-172.29.100.4	eth1.100	172.29.100.4/24	23	96%	23	9%
3		S-172.29.101.4	eth0.101	172.29.101.4/24	15	80%	15	6%
4		S-172.29.102.4	eth1.102	172.29.102.4/24	15	47%	15	6%
5		S-172.29.103.4	eth0.103	172.29.103.4/24	4	100%	4	2%
6		S-172.29.104.4	eth1.104	172.29.104.4/24	4	100%	4	2%
7		S-172.29.105.4	eth0.105	172.29.105.4/24	5	100%	5	2%
8		S-172.29.106.4	eth1.106	172.29.106.4/24	4	100%	4	2%
9		S-172.29.107.4	eth0.107	172.29.107.4/24	5	100%	5	2%
10		S-172.29.108.4	eth1.108	172.29.108.4/24	4	100%	4	2%

네트워크(센서) 별 IP 사용현황



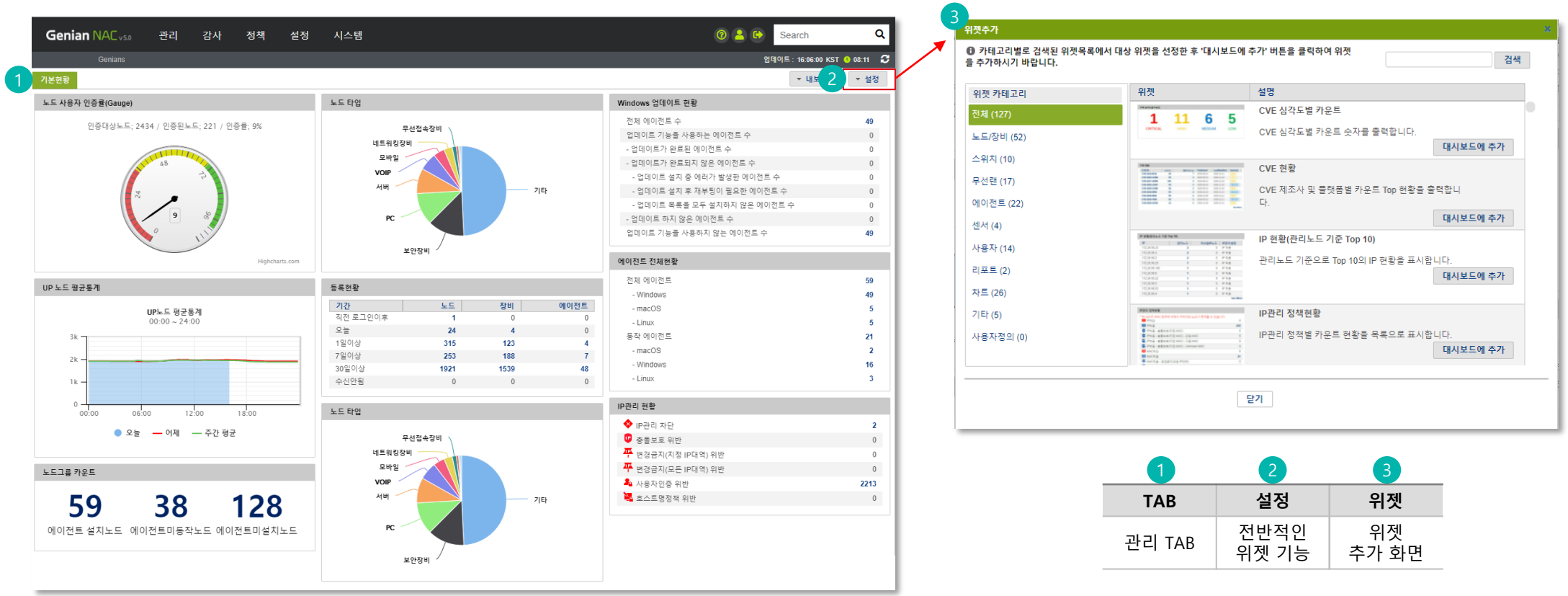
IP Matrix View

가시성 (Visibility)

Dashboard 를 통한 다양한 통계, 상태 등의 현황 파악 용이

대시보드는 Genian IPAM 의 메인 페이지로 관리자가 관심있는 항목에 대해 간단하고 가시성 있게 정보를 표현하여, 현황파악을 쉽게 할 수 있도록 함.

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



1	2	3
TAB	**설정**	**위젯**
관리 TAB	전반적인 위젯 기능	위젯 추가 화면

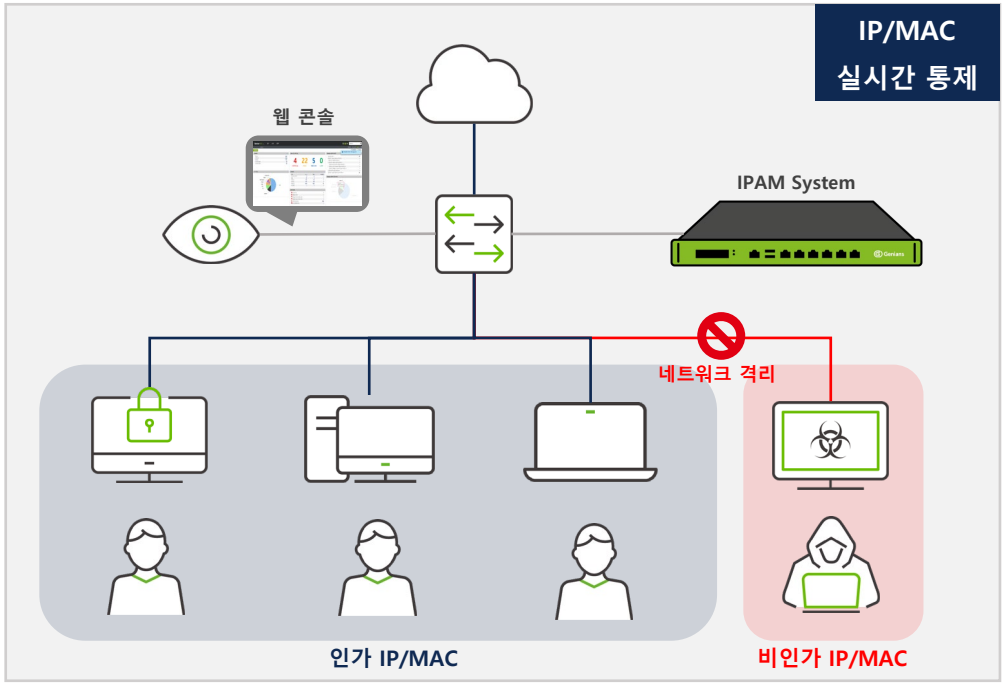
분류 (Classify)

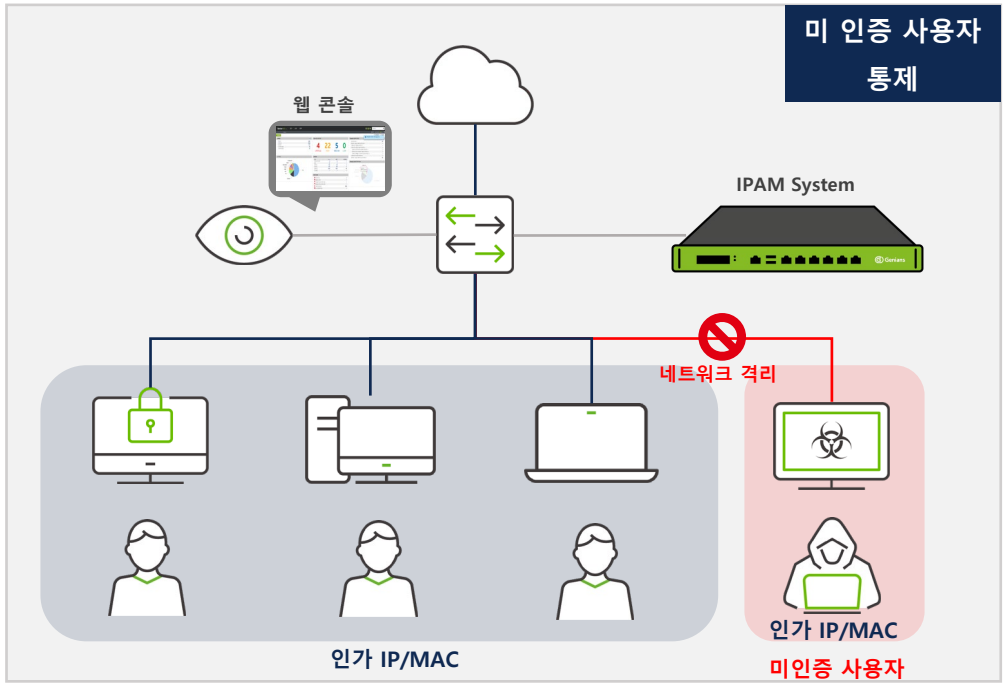
다양한 조건의 그룹 별 분류, 정보 확인 기능

통제 (Control)

네트워크 통제(Network Control)

- **전용 장비를 이용한 네트워크 통제 기능**
  - IP/MAC 실시간 확인 및 통제
  - 미 인증 통제
  - 방화벽 수준의 IP, Port, Protocol 기반 통제
  - 단말기 분류에 따른 통제





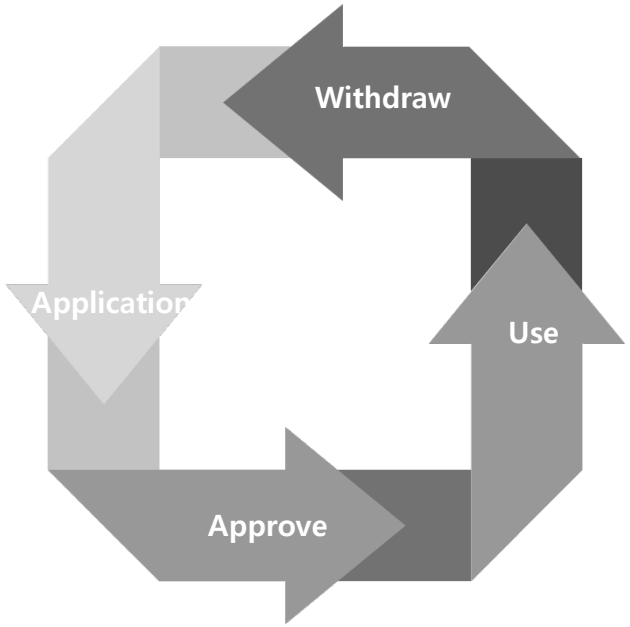
신청/승인

IP / 계정 사용 신청

신청
IP / 계정이 없는 사용자
신청 페이지를 통한 신청

Application

승인
신청 정보 확인 절차를 거쳐
승인



회수
사용 후 사용 기간 끝난
IP / 계정 삭제

사용
승인된 IP / 계정 네트워크
사용

신청/승인/사용/회수 이력 관리

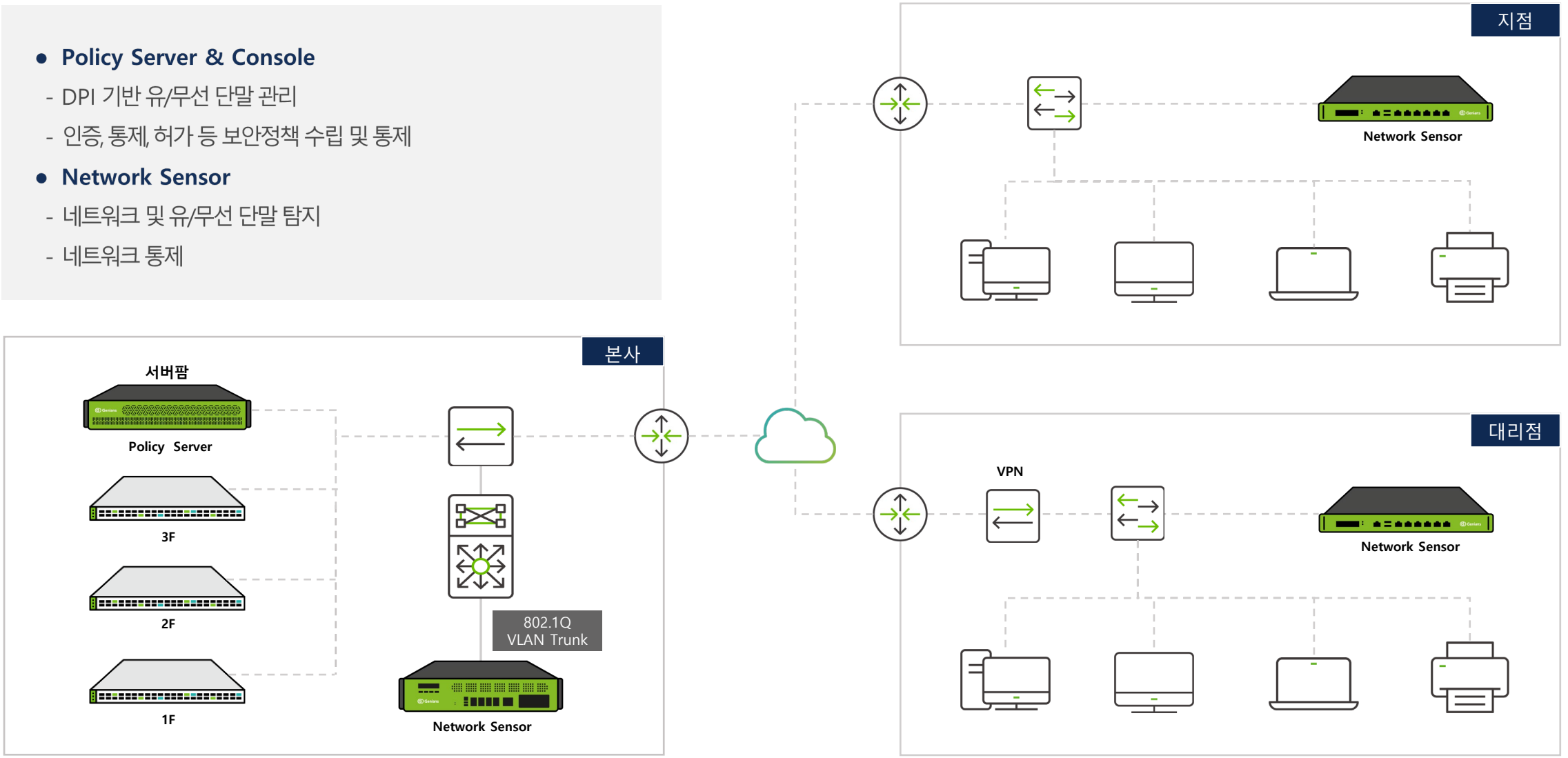
사용자 편의성

유연한 차단 페이지 구성(HTML)

- **전용 장비를 이용한 네트워크 통제 기능**
  - 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 IPAM 구성도

- **Policy Server & Console**
  - DPI 기반 유/무선 단말 관리
  - 인증, 통제, 허가 등 보안정책 수립 및 통제
- **Network Sensor**
  - 네트워크 및 유/무선 단말 탐지
  - 네트워크 통제



Genian IPAM 기능

IP 관리 기능 요약

IP 관리	실시간 IP/MAC 감지
	신규 IP/MAC 제어
	IP 충돌보호
	IP 변경금지
	IP 사용 시작시각/종료시각 제한
	MAC 사용 시작시각/종료시각 제한
	IP 사용 호스트명 제한
	IP 사용신청 시스템
	미사용IP 관리기능
	Matrix 뷰
	IP 고갈 경고

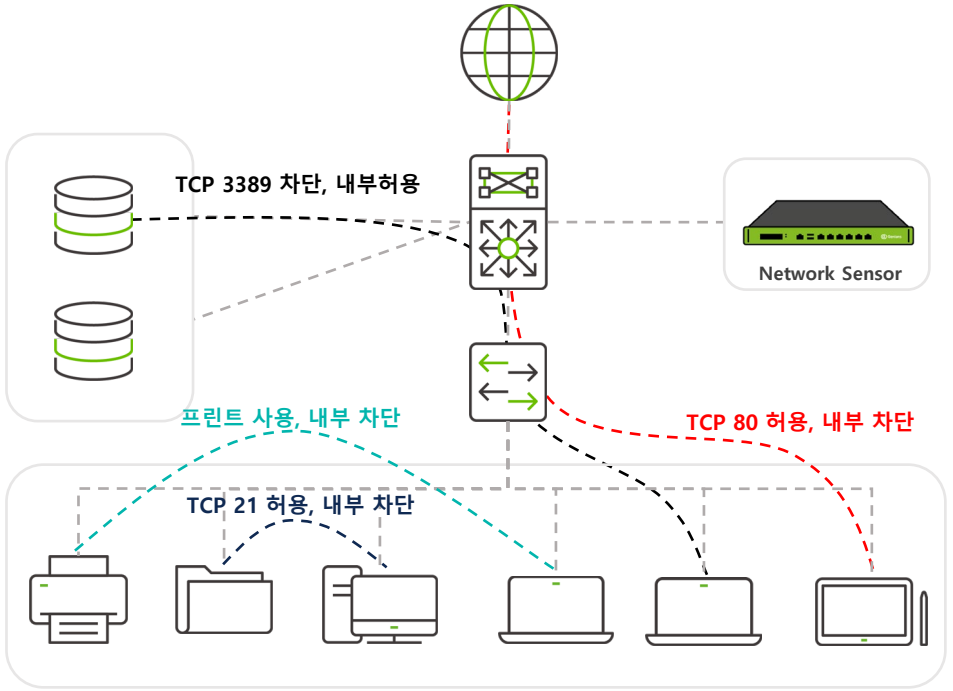
부가 기능

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	PC 열린 포트 정보
	사용자 PC 가 연결된 스위치 및 포트 정보
	Host 명, Domain 명
	PC 동작 유무 판단
DHCP	DHCP 서비스 제공
	IP Pool 기능
로그	IP 이력 현황 및 기타 로그 관리

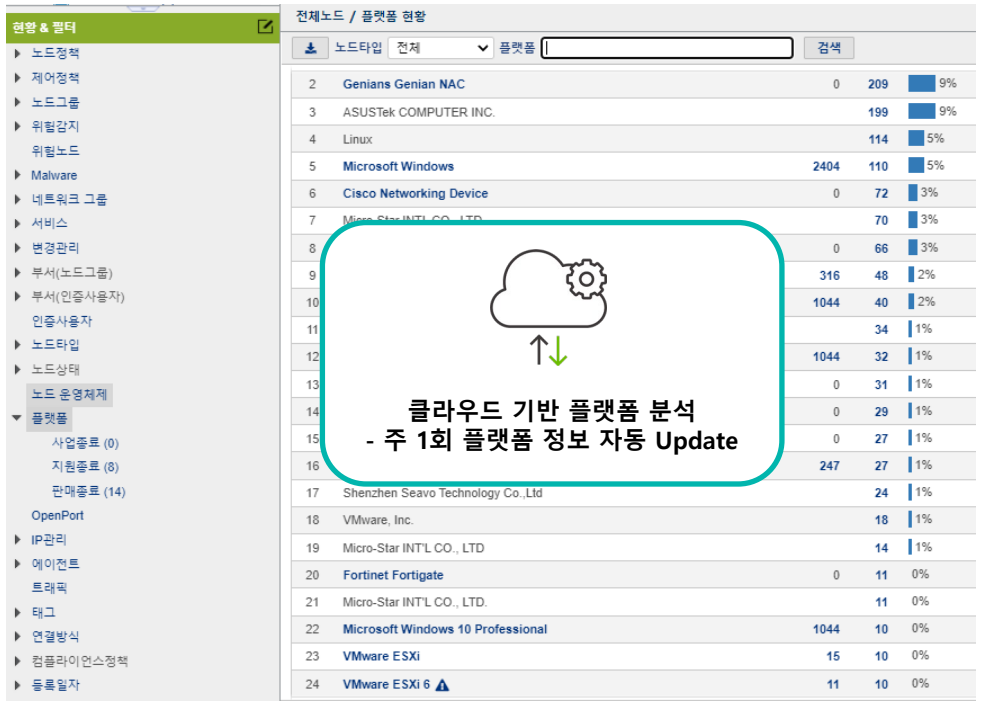
Genian IPAM 특/장점

최고의 기술력을 바탕으로 한 안정성과 다양한 기능

- **방화벽 기반의 IPAM**
  - Agent 와 무관한 네트워크 제어
  - 방화벽 수준의 IP, Port, Protocol 제어 기능 제공
  - PC 가 아닌 모든 장치에 대한 네트워크 통제 가능



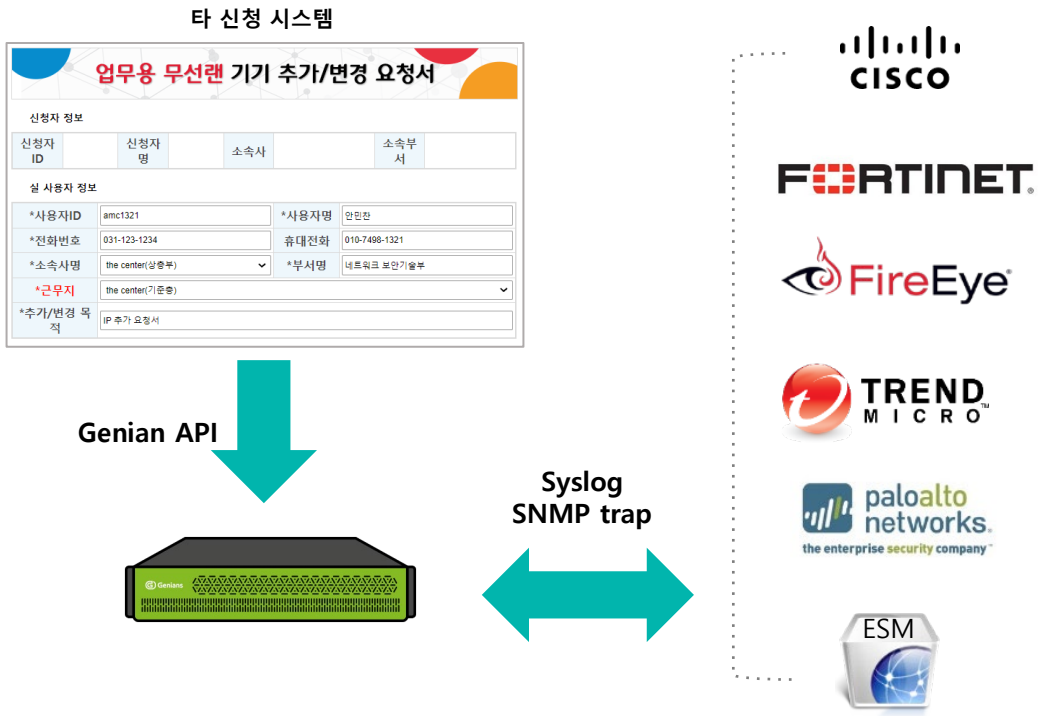
- **IPAM 필수 조건인 가시성 확보를 위한 기능**
  - 플랫폼 DB 를 통한 장치 구분 및 플랫폼 자동 분류
  - Agent 설치 없이 OS 버전, 모델명 등 자동 분류
  - 신규 장치에 대한 cloud 형태의 자동 업데이트 기능 제공



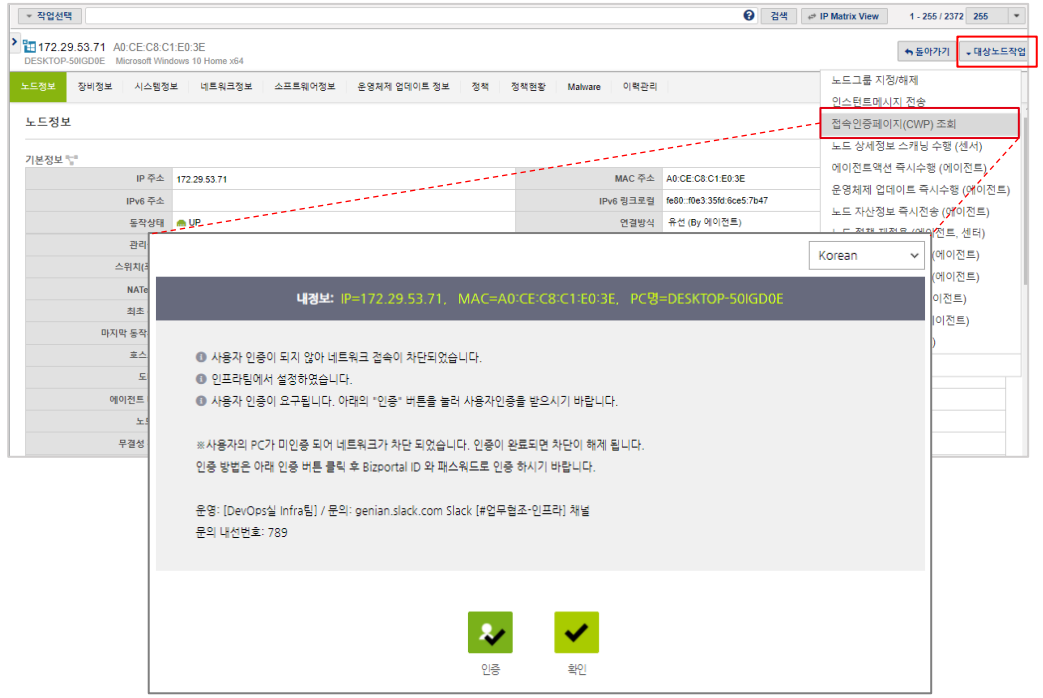
Genian IPAM 특/장점

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
  - IPAM 자체 API 를 이용한 타 시스템과의 연동을 통한 자동화 구현



- **차단 페이지 시뮬레이션 기능**
  - 관리자 콘솔을 통해 사용자의 차단 페이지 가상 확인 기능 제공



03. 지니언스 회사소개

회사개요

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

Genians
지니언스

회 사 명	Genians ㈜
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, 단말 이상행위 탐지 및 대응 솔루션 개발/판매 정보보안 수준 진단 및 평가 솔루션 개발/판매
임 직 원 수	149명 (21년 10월 현재)
협 력 사	론스텍(총판), 대신정보통신(총판) 등 약 30개사
주 소	경기도 안양시 동안구 벌말로 66 평촌역 하이필드 지식산업센터 A동 12층
홈 페 이 지	https://www.genians.co.kr/

THANK YOU :)

Genians