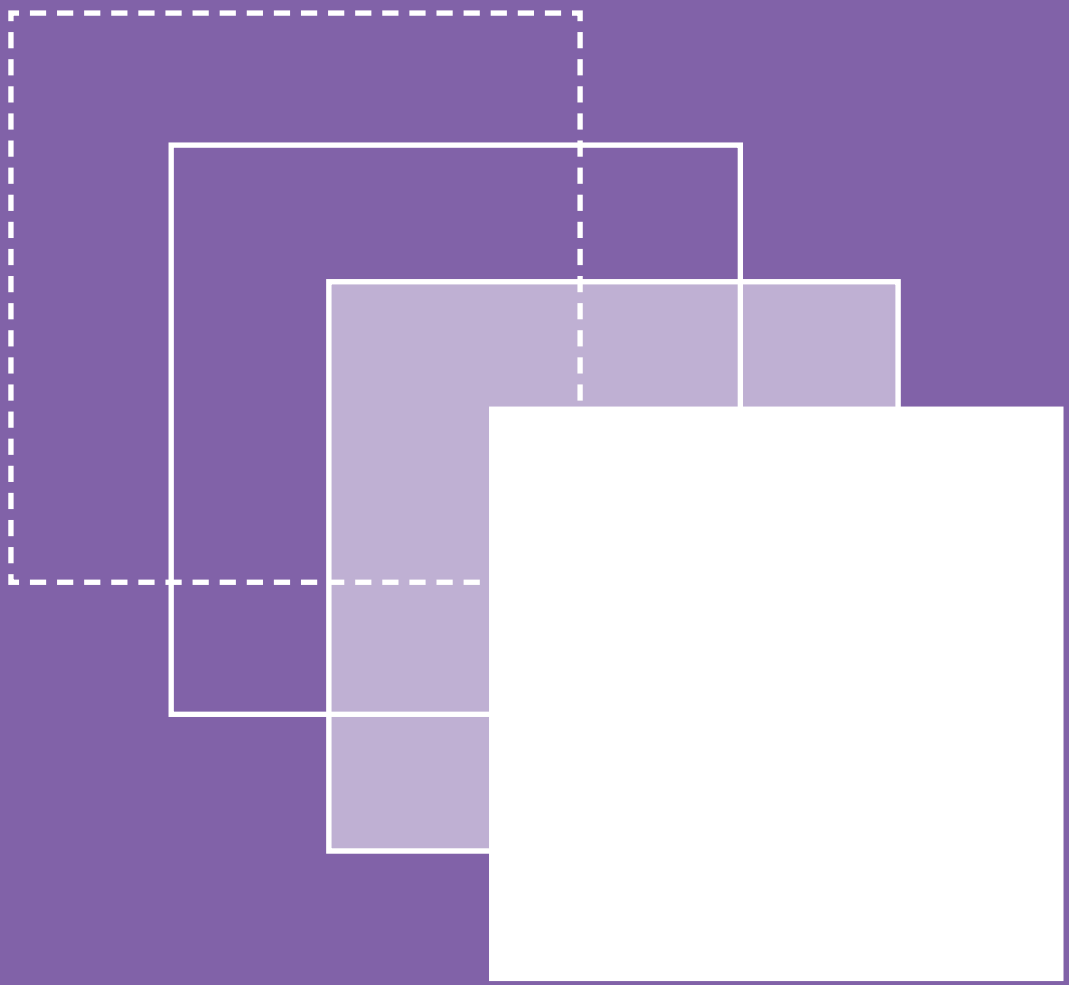
제로트러스트 기반 네트워크 접근 제어 솔루션

Genian ZTNA

v 6.0



Genians

Genian ZTNA

개요
Overview

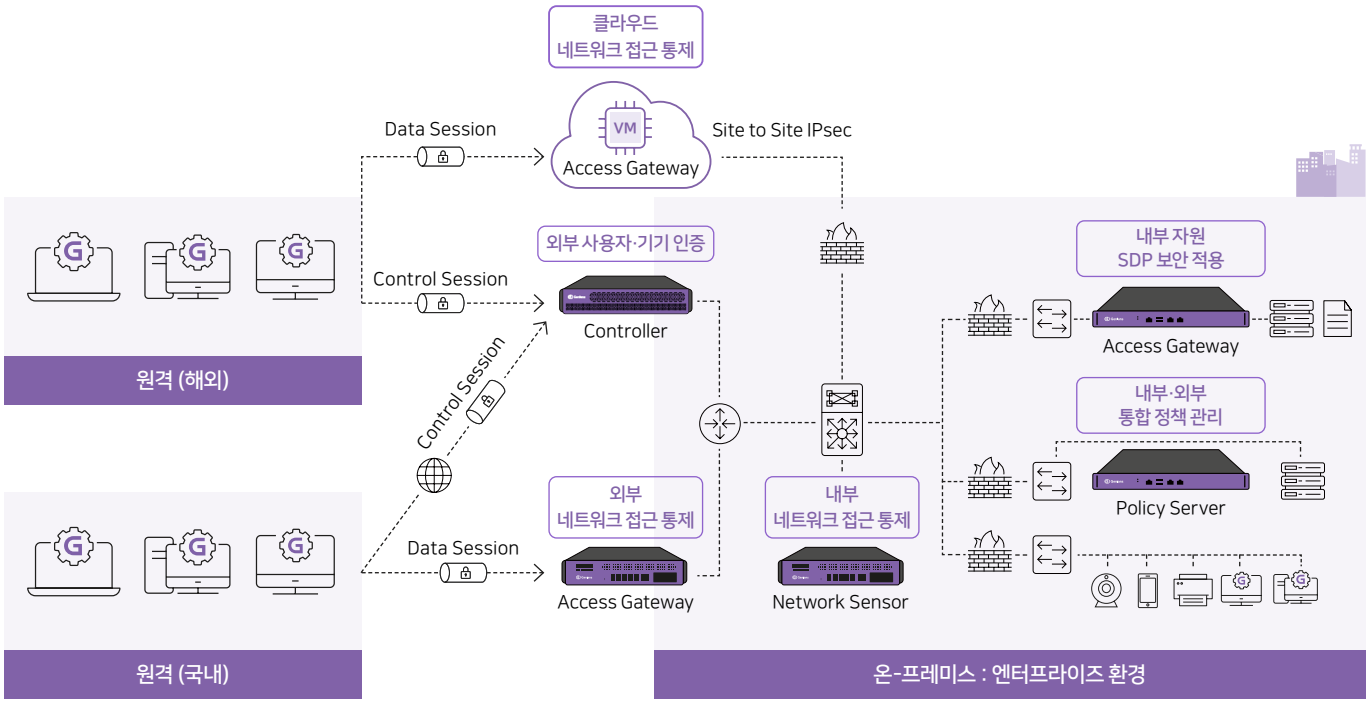
디지털 전환과 클라우드 확산으로 내부와 외부의 경계가 사라지면서, 기존 NAC만으로는 새로운 보안 요구에 대응하기 어려운 한계가 드러났습니다. 특히 원격 근무, 다양한 기기와 애플리케이션 사용이 일상화되면서 보다 정교하고 지속적인 검증이 필요해졌습니다. 지니언스는 이러한 환경 변화를 반영해 NAC의 강점을 확장하고, 네트워크·사용자·애플리케이션 전반을 아우르는 보안 체계로 발전시켰습니다.

Genian ZTNA는 변화된 환경에 최적화된 차세대 보안 플랫폼입니다.
"Never Trust, Always Verify" 원칙을 기반으로, 사용자와 기기, 그리고 애플리케이션을 지속적으로 검증하여 세밀한 접근 제어를 제공합니다.

- **에이전트 기반·비에이전트 기반 접근 제어를 모두 지원하여 다양한 환경에 유연하게 대응합니다.**
- **단일 정책 프레임워크를 통해 내부망, 원격, 클라우드 환경 모두에서 일관된 보안 정책을 적용합니다.**
- **실시간 단말 보안 상태 검사와 동적 세션 제어를 통해 위험 발생 시 즉시 접근을 차단합니다.**
- **클라우드·온프레미스 동시 지원으로 고객 환경에 맞춘 유연한 배포가 가능합니다.**

아키텍처
Architecture

Genian ZTNA는 단순히 네트워크 경계를 대체하는 것이 아니라, 사용자·단말·애플리케이션 중심의 새로운 보안 체계를 구축하여 디지털 전환 시대의 비즈니스 연속성과 안전한 성장에 기여합니다.



도입효과
Benefit of ZTNA

통합 관리의 단순화	즉각적인 보안 대응	투자 비용 절감
사무실, 클라우드, 원격 근무자를 통합 관리하므로 일관성 있는 보안 정책과 지속적인 모니터링을 통해 컴플라이언스를 유지하고 감사 기록합니다.	제로트러스트로의 전환은 사회적 이슈나 환경의 변화 등 어떠한 상황에도 보안을 지속적으로 유지할 수 있으며, 위협에 따른 대응과 통제가 즉시 이루어집니다.	디지털 전환으로 사람, 자산의 경계가 사라졌습니다. 곳곳에 보안 솔루션을 배치할 때 발생되는 비용 부담을 제로트러스트의 전환으로 절감할 수 있습니다.

Product Function

통합 보안(관리)을 위한 다양한 핵심 기능 제공

네트워크 접근 제어

- 속성 기반 접근 통제(ABAC: Attribute-Based Access Control)
- 표준 802.1X 지원(RADIUS) 및 Dynamic Vlan제공
- DHCP 내장 및 할당 제어
- ARP 기반 Layer 2 지원
- 포트 미러링 및 방화벽/스위치 통합 기반 제어

사용자 인증 관리

- 자체 포털(CWP) 사용자 인증 지원
- 기존 인사 DB 및 타 솔루션 인증 연동
- AD(Active Directory) 인증 연동(SSO)
- 802.1X 기반 RADIUS 제공 및 Dynamic Vlan지원
- LDAP, SMTP, POP3, IMAP 등 외부 인증 연동
- SAML(Google G Suite, Okta, Azure) 인증 연동
- 지문인식 및 OTP(Google OTP 등) 연동

IP 관리

- 독립 솔루션 수준의 IP 관리 기능 제공
- IP/MAC 제어(사용 시간, 사전 예약 등)
- IP/MAC 충돌 보호/변경 금지
- IP/MAC 스푸핑(Spoofing) 감지
- DHCP 제공 및 IP 신청/승인 등 업무절차 지원
- 인사 DB 연동을 통한 IP 실명제 및 이력 관리
- 감사 대비 자료 제출용 이력 정보 추출 기능 제공

패치 및 소프트웨어 관리

- WSUS 기반 MS Windows 및 Office 패치 관리
- 패치 적용 시점 및 백그라운드 설치
- 패치 설치 대상 및 승인 여부 관리
- 독립 배포 서버 구축(폐쇄망 및 오프라인 패치 지원)
- 관리자 지정 소프트웨어 배포 및 설치(백신 등)
- 규정 위반 소프트웨어에 대한 원격/강제 삭제 등
- 일반 파일 배포 및 설치 지원

무선 네트워크 접근 제어

- SSID별 접속 단말 현황 파악
- 사용자 기반 AP 위치 정보 제공
- 불법(Rogue) AP 탐지 및 유선/에이전트를 통한 전방위 통제
- SoftAP/Adhoc/Hidden SSID 등 다양한 무선랜 정보 제공
- 무선 접속 매니저(EAP-GTC) 제공 및 802.1X 지원

자산 관리(DMS)

- DPI(Device Platform Intelligence) 기반 단말 상세 정보 제공 (단말 종류, 운영체제 정보, EOL/EOS, CVE 등)
- 600여 가지 조건에 따른 단말 자동 분류
- 단말 변경 사항 추적/감사 등
- Agent 기반 H/W 및 S/W 상세 정보 수집 및 관리

3rd Party 제품 연동

- WorkFlow를 통한 운영 간소화 및 보안 자동화 지원
- RESTful API, Syslog, Webhook, SNMP Trap 등 지원
- CISCO/ORACLE/MYSQL/DB2/Tibero/Altibase/CSV 등 연동
- V3 등 백신 및 Palo Alto Networks, FireEye 제품과 연동

거버넌스 관리

- 노드에 대한 보안 등급(기밀/민감/공개) 관리
- 노드 그룹별 위험 등급(심각/높음/중간/낮음) 관리
- 보안 등급 및 위험 등급에 대한 현황 및 모니터링 제공

기타/일반 관리

- 이중화 구성 지원(Policy Server/Network Sensor/ Controller/Gateway)
- 150가지 이상 위젯(Widget) 기반의 대시보드 지원
- 기본 리포트 및 고객 맞춤형 리포트 제공
- 다국어 지원(한국어/영어/일어/중어)

ZTNA License (Option)

클라우드 환경 및 구성 지원 (AWS,Azure, Google, Naver 등)

- 클라우드에 배포된 자원에 대한 가시성 및 정보 제공
- 클라우드 보안 그룹 정책 관리 지원
- 클라우드 Access Gateway 원 클릭 설치 지원
- AWS CLI 명령 도구를 통한 클라우드 제어

재택 근무 인프라 지원

- NAC 및 VPN 통합 에이전트 제공
- 원격 접속을 위한 SSL VPN 및 Client 기능 제공
- 원격 접속 간 분할 터널링 기능 제공
- 사용자, 단말, 애플리케이션 기반 세분화된 접근 정책 지원

Product Function

보안 통제
Security Control

제로트러스트 기반으로 모든 접근과 행위를 지속적으로 검증하며, 보안 정책 위반에 대해 다양한 대응 방안을 제공합니다. 사용자 권고, 대응 및 예방 조치를 동시 수행해 보안 관리의 효율을 극대화합니다.

알림 (Alarm)

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

차단 (Block)

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

교정 (Remediation)

- **필수 S/W 설치 유도**
  (백신, DRM, DLP 등 보안 솔루션 강제 설치)
- **불법 S/W 삭제**
  (허용되지 않은 특정 S/W 강제 삭제)
- **보안 설정 강제화**
  (패스워드 설정, 화면 보호기 등)

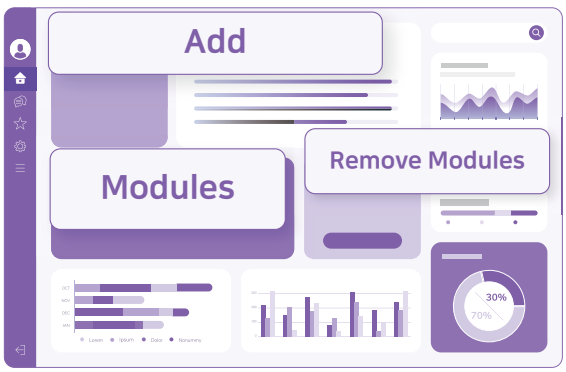
통합 에이전트
Unified Agent

에이전트 설치 유/무에 따라 단말 내부의 상세 정보 수집 및 제어의 범위가 다릅니다. 에이전트 설치는 조직의 보안 정책 및 관리 수준에 따라 선택적 적용이 가능합니다.

Agent-less

* Agent 없는 환경에서도 다양한 방식으로 접근 제어

구분	세부 정보
플랫폼 분류	· OS (Windows, Linux, Unix, iOS, Android 등), 네트워크 장비, 프린터, 제조사 등
접근 제어	· IP, MAC, Port, Protocol별 접근 제어 · 플랫폼별 접근 제어 (OS 및 장치별) · 시간/요일/기간 접근 제어 · 사용자별 접근 제어 (인증/미인증, ID, 부서, 직급 등)
네트워크 정보	· IP 관리 (IP/MAC 고정, 변경 금지, 충돌 보호, 사용 시간 등) · 사용자 PC가 연결된 스위치 및 포트 정보 · 호스트명, 도메인명 · PC 동작 유무 판단, PC 열린 포트 정보



Agent

* Agent 기능 모듈화로 단말 리소스 최적화 및 유지보수 용이

구분	세부 정보	OS
장치 제어	· USB, NIC, Bluetooth, Wifi, Tethering, PC전원 제어	
포트 정보	· 열린 포트, 포트 사용 프로세스, 서비스 정보	
백신 연동	· 백신(V3, 바이로봇, 알약) 업데이트 및 바이러스 탐지에 대한 네트워크 제어	
행위 판단 제어	· 트래픽 정보 및 TCP 세션 정보 수집, 임계치 초과 시 차단	
위변조 탐지	· IP, MAC clone 탐지/차단	
보안 기능	· 자동 실행 제어, 웹 브라우저 옵션 제어, 계정 취약성 검사	
	· 무선랜 제어, 호스트명 변경, 프린터 정보 수집, 인터페이스 제어	
	· 프로그램 제거	
	· 비밀번호 유효성 검사, 화면 보호기 제어, 공유 폴더 제어, 네트워크 우회 접속 방지, ARP Spoofing 방지, OS 보안 설정, OS 방화벽 제어, 파일 배포, 웹 브라우저 보안 설정, 에이전트 인증 창	
OS 패치	· OS Patch(Windows, MacOS, Linux PMS) 기능 제공	
프로세스 제어	· 특정 프로세스 강제 종료	
소프트웨어 탐지	· 필수 S/W, 불법 S/W 탐지 및 제어	
메시지 전송	· 사용자에게 메시지 전송 (공지 및 알림 팝업)	
시스템 정보	· PC OS 및 H/W 정보(CPU, MEM, DISK, NIC 등), 호스트명 수집 및 제어	

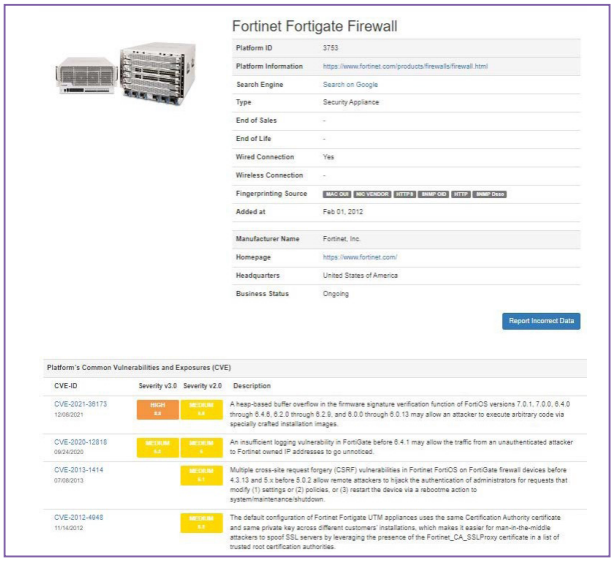
Key Features

확장된 가시성
Enhanced Visibility

DPI는 네트워크에 연결된 IT 자산(단말 등) 및 OT 자산을 실시간으로 탐지하여 식별하고 상세하게 분류합니다. 단말의 일반 정보는 물론 확장 정보와 취약점 정보까지 제공하여 생명주기 관리까지 업무 영역을 확대할 수 있습니다. 일반 IT 환경뿐 아니라 공장, 설비 등의 OT 환경에서도 적용 가능합니다.

구분	세부 정보
단말 식별 정보 (Device Identity)	· 단말 제조사, 이름, 모델 번호 · 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)

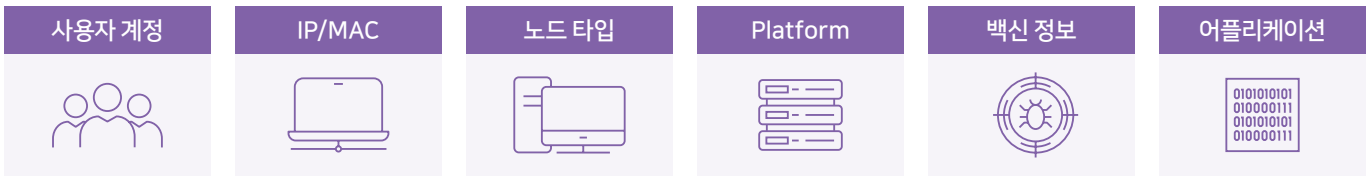
DPI가 제공하는 단말 관련 정보



DPI를 이용한 'Fortinet' 단말 확인

세분화된 정책
Micro Segmentation

ZTNA는 내·외부 구분 없는 조건 기반 정책을 통해 모든 접속 환경에서 일관된 보안을 제공합니다.



600여 가지 이상의 조건식(AND & OR) 기반 정책 생성

사용자	규정 정책	권한 정책							
		접속 위치	자산 유형	플랫폼	업무 시간	허용 서비스		허용 어플리케이션	
일반 사용자	IP 관리 정책 기본 보안 설정 필수 소프트웨어 보안 패치	사무실	PC	Windows	평일 09:00-18:00	그룹웨어 파일서버	192.168.10.10:443 192.168.10.11:80	ERP	www.erp.com www.erp.com/home
시스템 관리자		재택	PC	mac OS Windows	상시 00:00-24:00	그룹웨어 파일서버	10.22.10.10:3389 10.22.11:22	ITSM	www.itsm.com www.itsm.com/home

간편한 통합
Seamless Integration

다양한 3rd Party 솔루션과 연동하기 위한 표준화된 인터페이스와 통합 기능을 제공합니다.

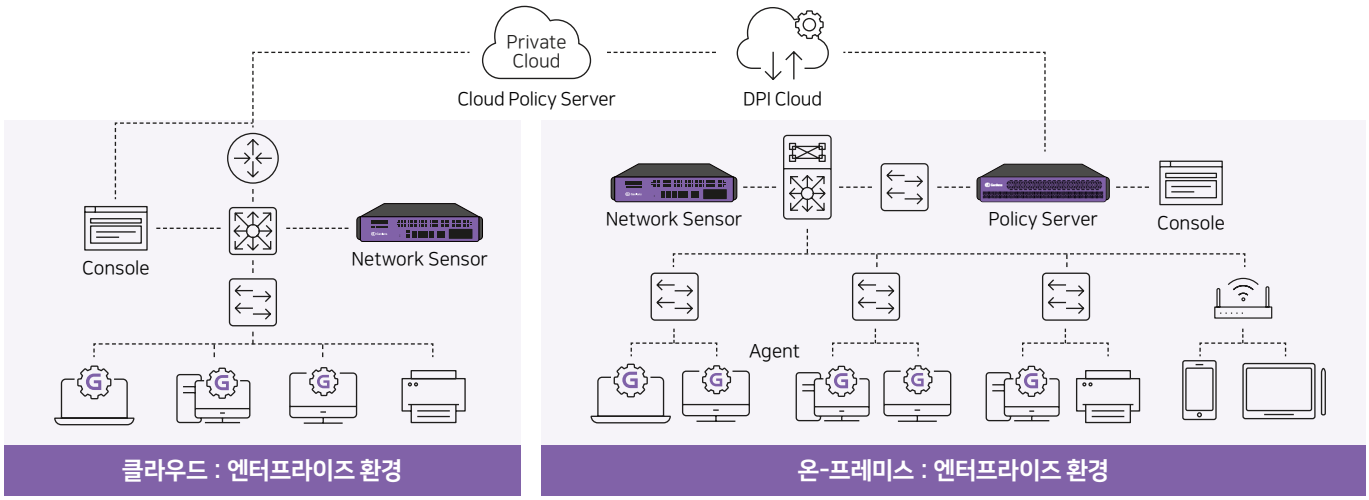
Operating Mode

구성 방안
Configuration Overview

Genian ZTNA는 형태 및 목적에 따른 다양한 설치 및 운영 방법을 제공합니다.

On-Premise (구축형)	Cloud (SaaS)	VM (가상 머신 등)
· 기관 및 기업의 독자적인 운영 가능 · 국내 환경에 가장 적합 · 고객사에서 가장 선호하는 형태	· 국내 보안 솔루션 최초 클라우드 서비스 보안인증(CSAP)을 받은 제품	· 서비스 사업자를 위한 (MSP, MSSP, CSP, SaaS 등) 다양한 플랫폼 및 운영 환경 지원 · VM, uCPE, WhiteLabeld 등 포함

On-Premise (구축형) 내부 구성도
On-Premise Internal Diagram



클라우드 : 엔터프라이즈 환경 | 온-프레미스 : 엔터프라이즈 환경

Component	Main Features	Specifications
Policy Server & Console	· DPI 기반 유/무선 단말 관리 · 인증, 통제, 허가 등 보안 정책 수립 및 통제	· 범용 OS(이중화 및 DB 분리 구성 지원) · 전용 어플라이언스 외 클라우드 환경 지원 · COTS(Commercial off-the-shelf), VM, Docker 등 지원 · 표준 브라우저 지원(Chrome, Firefox, Safari 등)
Network Sensor	· 네트워크 및 유/무선 탐지 · 네트워크 통제	· 유선 : 범용 OS(이중화(HA) 구성 지원) · 802.1Q, 802.1ad, Bonding Port 지원/In-Line 지원 · 전용 어플라이언스 외 클라우드 환경 지원, COTS, VMuCPE(Universal Customer Premise Equipment) 등 지원
Agent (Option)	· 단말에 설치되어 정보 수집 및 장치(USB 등) 사용 통제 · 비용 부담 없으며 선택적 사용	· Windows, mac OS, Linux 환경 지원

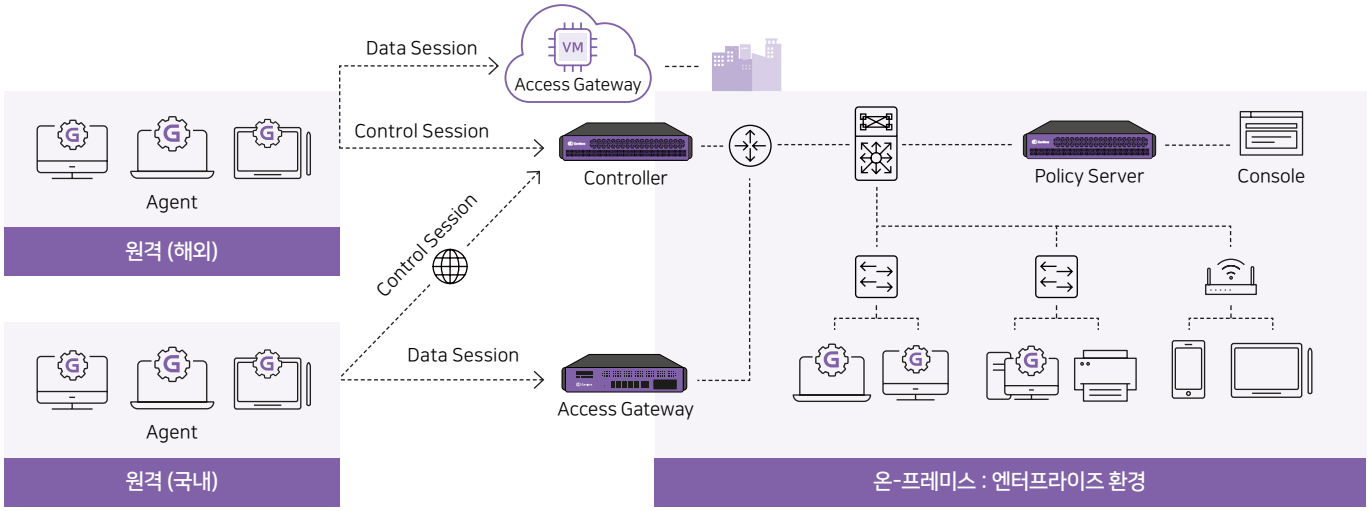
운영 환경
Operating Environment

구분	Policy Server (정책서버)	Network Sensor(차단센서)	Agent (에이전트)	Console (콘솔)
사양	· 전용 어플라이언스(범용 OS)	· 전용 어플라이언스(범용 OS)	· Windows 8.1 이상 · mac OS Big sur 11.0 이상 · Linux(Debian, RedHat)	· MS Edge 40.x 이상 · Chrome 75.x 이상 · Firefox 14.x 이상 · Safari 12.x 이상 · IE 10.X 이상

Operating Mode

On-Premise(구축형) 외부 구성도

On-Premise External Diagram

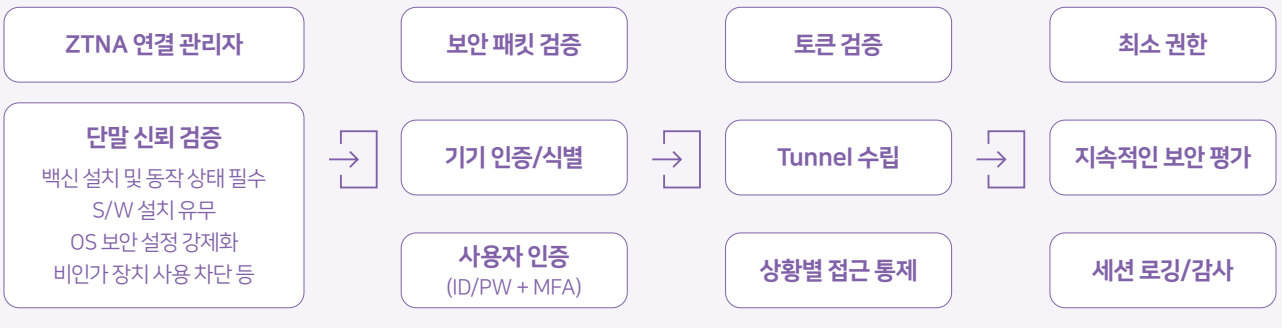


Component	Main Features	Specifications
Controller (Option)	· SDP 보안 아키텍처 지원 · 외부 사용자 및 기기 인증 · 외부 사용자 서비스 간 연결 제어 · SDP 구성 필요에 따라 선택적 사용	· 범용 OS 기반 이중화(HA) 구성 지원 · 전용 어플라이언스, VM, 클라우드 환경(AWS 등) · COTS(Commercial Off-The-Shelf) 및 Docker 환경 지원
Access Gateway	· SSL VPN 기능 제공 · 외부 네트워크 접근 통제 · 애플리케이션 인지 및 통제	· 범용 OS 기반 이중화(HA) 구성 지원 · 서비스 트래픽에 대한 인라인/프록시 모드 지원 · 전용 어플라이언스, VM, 클라우드 기반 구축 가능 · DPI 기반 애플리케이션 인식 및 제어 기능 포함
Agent	· SSL Client 접속 기능 제공 · 단말에 설치되어 정보 수집 및 장치 사용 통제	· Windows 8.1 이상 · mac OS Big sur 11.0 이상 · Linux (Debian, RedHat)

소프트웨어 정의 경계

Software Defined Perimeter

소프트웨어 정의 경계는 제로트러스트 핵심 원칙 중 하나입니다. ZTNA는 외부 사용자의 안전한 네트워크 접속을 위해 소프트웨어 정의 경계 기법을 지원합니다.



조달 디지털서비스몰

NAC 물품식별번호

NAC Product Identification Number

다량납품 할인율
- 350,000,000 이상 2.5% 할인
- 500,000,000 이상 5% 할인

제품군	규격 명	조달 단가	물품식별번호
Node License	Genian ZTNA V6.0 SP1, 1~500Node, Enterprise Node License	64,900	25533812
	Genian ZTNA V6.0 SP1, 501~1000Node, Enterprise Node License	44,000	25533813
	Genian ZTNA V6.0 SP1, 1001Node이상, Enterprise Node License	22,000	25533814
정책서버 모듈	Genian ZTNA V6.0 SP1, 1~1000Node, 정책서버모듈	8,800,000	25533802
	Genian ZTNA V6.0 SP1, 1~5000Node, 정책서버모듈	15,400,000	25533803
	Genian ZTNA V6.0 SP1, 1~10000Node, 정책서버모듈	20,900,000	25533804
차단센서 모듈	Genian ZTNA V6.0 SP1, 1~150Node, 차단센서모듈	3,300,000	25533805
	Genian ZTNA V6.0 SP1, 1~500Node, 차단센서모듈	6,600,000	25533806
	Genian ZTNA V6.0 SP1, 1~1000Node, 차단센서모듈	15,400,000	25533807
	Genian ZTNA V6.0 SP1, 1~2000Node, 차단센서모듈	24,200,000	25533808

* IPAM 구매 시 제조사에게 별도 문의 필요
* 조달청 디지털서비스몰: https://digitalmall.g2b.go.kr

14058 경기도 안양시 동안구 벌말로 66 평촌역 하이필드 지식산업센터 A동 12층
기술지원 : 1600-9750 (평일 오전 9시~오후 6시) / 도입문의 : sales@genians.com

Genians