통합 보안 플랫폼 기업, 지니언스

# Genian ZTNA v6.0

# 제품 소개서

Genians

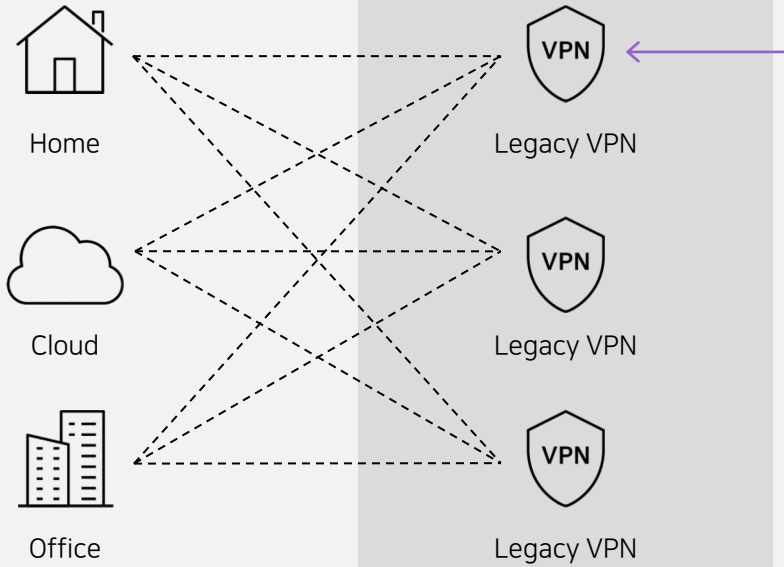
01

# 배경 및 필요성

# 기업의 업무 환경 변화

## 통제 영역을 벗어난 새로운 업무 환경의 추가에 따른 고려사항 발생

환경 변화 → 대응 수단 → 보안 문제 → 관리부서의 고민




일회성 신뢰 확인

전체 네트워크 액세스

관리의 어려움

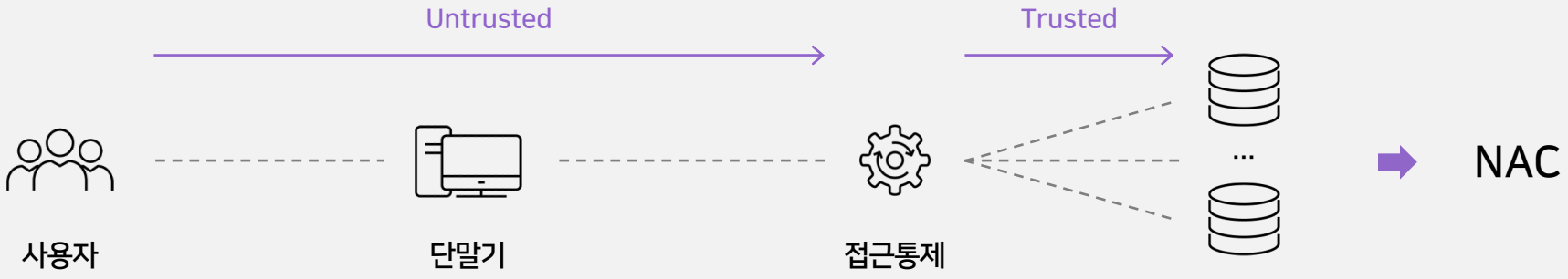
클라우드 통제 부재

- 사용자 인증 강화
- 단말의 보안 상태
- 사용자/단말 가시성
- 상태 변화에 따른 통제
- 클라우드 접근 통제
- 최소 권한 액세스

# 새로운 보안전략 '제로트러스트'

## 변화된 업무 환경에 대응 하기 위한 새로운 보안 전략의 필요성

### 제로트러스트 데이터 접근 흐름




- 등록된 사용자가 맞나?
- 회사 소유의 단말인가?
- 사내 보안 기준을 만족하나?
- 사용자 Role-Base 접근 통제
- 단말별 접근 통제
- 필수 소프트웨어 통제
- 올바른 응용 프로그램 접근 권한을 가지고 있나?

### ZTNA로의 확장

1. NAC는 차세대 접근 통제 기술인 ZTN(Zero Trust Network)의 핵심

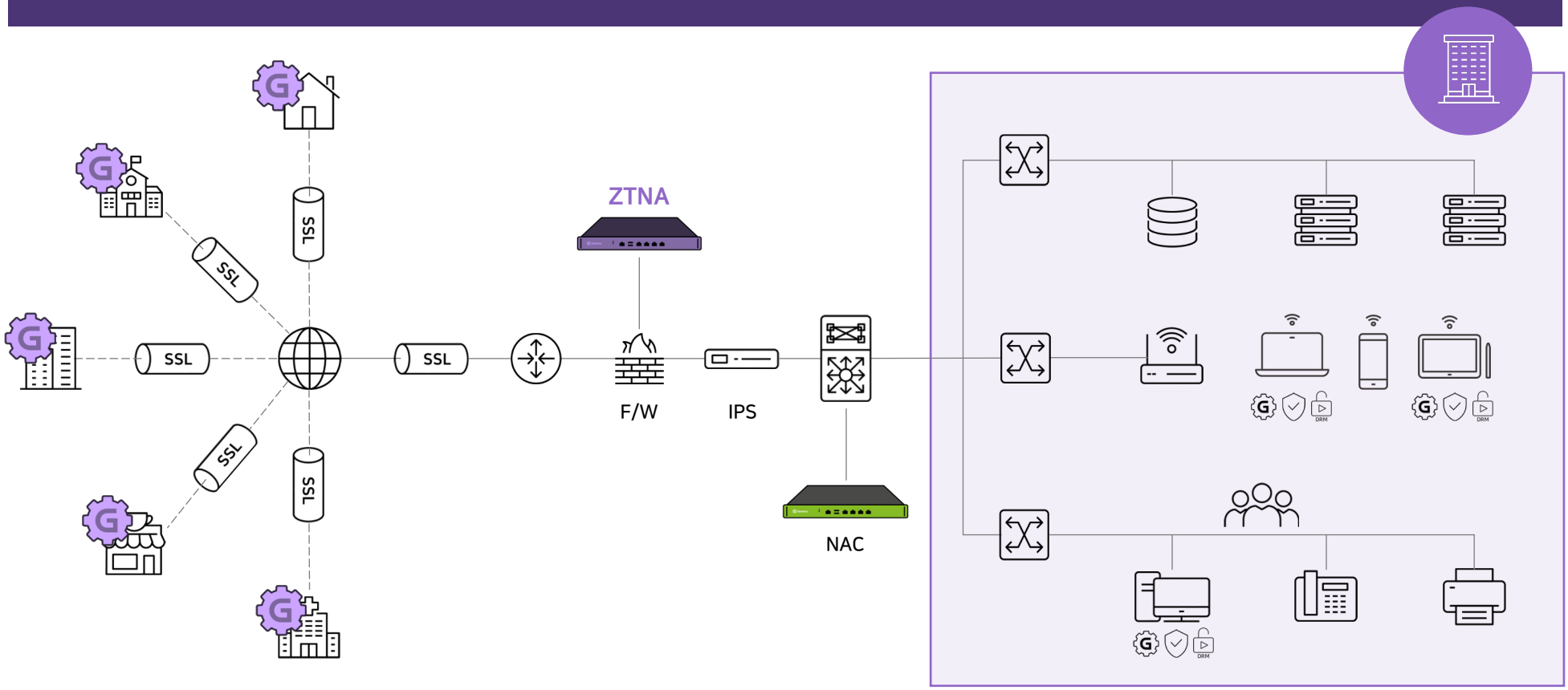
<By Gartner, Frost & Sullivan Market report>

2. 보안의 기본 'NAC', 차세대 ZTNA 근간으로 재조명

<By 컴퓨터월드 등 다수의 국내 보안 매체>

# ZTNA 통제 영역

## ZTNA는 원격지와 클라우드 영역까지 통제 영역 확대




새로운 업무 환경에 맞는 **Genian NAC의 확장**, 이것이 Genian ZTNA의 핵심

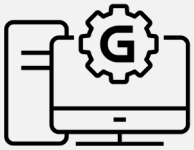
02

# Genian ZTNA 제품 소개

# ZTNA 구성 및 역할

## 제로트러스트 아키텍처 구현을 위한 신규 기능 및 구성 제공

### ZTNA Agent

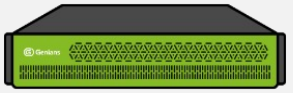


- SSL Client 로 안전한 원격 접속 제공
- MFA 통한 강력한 사용자 인증
  - FIDO 인증 표준의 PassKey
  - Google OTP, SMS, Webhook
- Kill Switch를 통한 인터넷 접속 제한
- 실시간 단말 Compliance 검증
- NAC 및 VPN Client 통합 Agent 지원

### ZTNA G/W


- SSL VPN, IPsec
- 장치 인증
- 어플리케이션 통제
- Container 기반 유연한 환경구성
- 실시간 동적 접근 통제
- Split, Non-Split Tunnel 지원
- IP-Mobility(지원 예정)

### ZTNA Policy

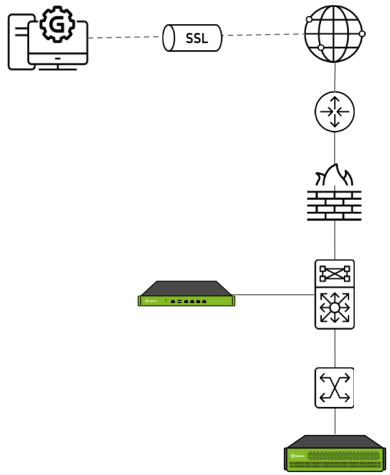


- 제로트러스트 정책 수립 및 관리
- 연동 API 지원
- SSO 인증 연계 지원
- 클라우드 보안 그룹 관리
- 클라우드 및 네트워크 가시성
- IDP(지원 예정)

# ZTNA 구성(1/2)

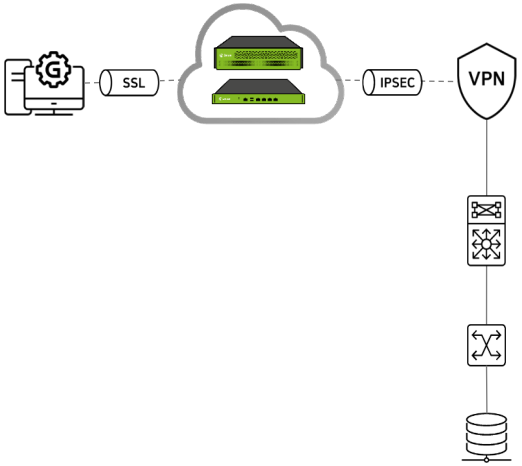
## 클라우드 / 온-프레미스 / 하이브리드 환경 구성 지원

### ON-Prem



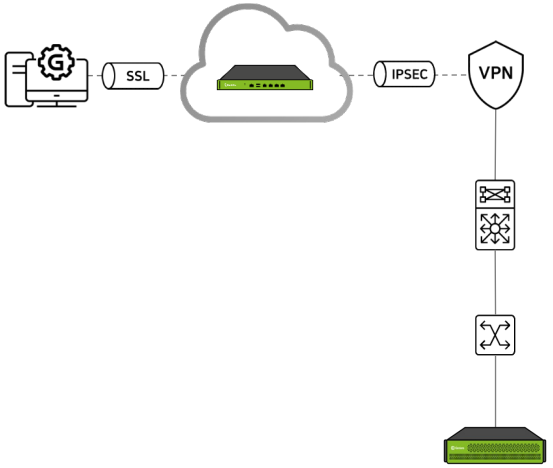

내부망에 ZTNA Policy, ZTNA Gateway 를 구성하는 방식

### Cloud




Cloud에 ZTNA Policy, ZTNA Gateway 를 모두 구성하는 방식

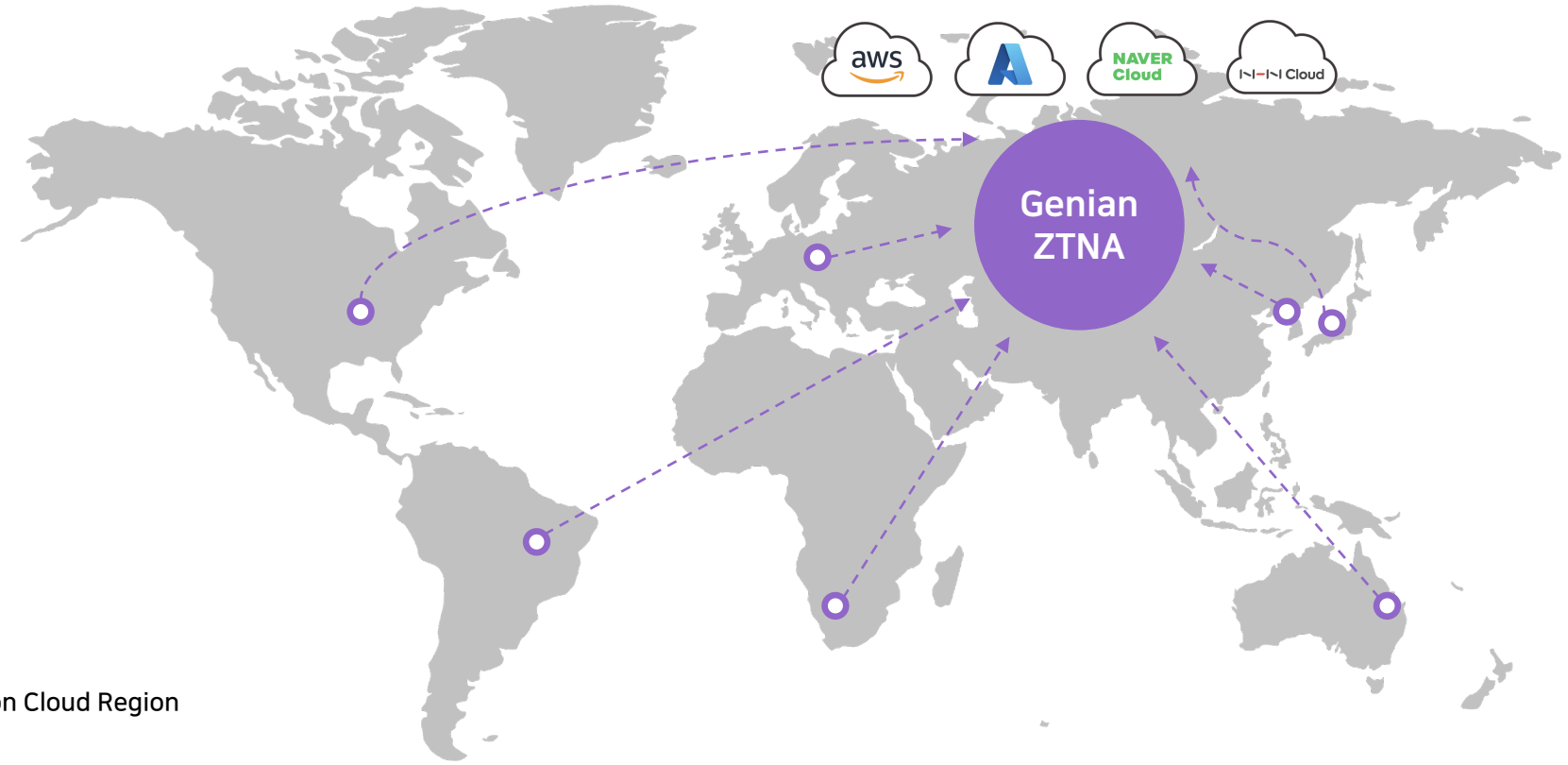
### Hybrid




Cloud에 ZTNA Gateway 를 구성하고 On-prem 환경에 ZTNA Policy 를 구성하는 방식

# ZTNA 구성(2/2)

## 멀티 클라우드 환경에 ZTNA Gateway 자동 구성 지원으로 즉각적인 보안 대응 실현




* Amazon Cloud Region

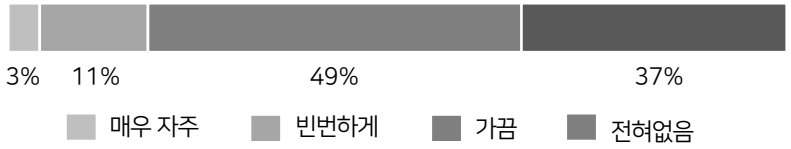
## 빠르고 쉬운 ZTNA Gateway 구성

# ZTNA 인증(1/2)

## 비밀번호 없이 로그인‥ 패스키로 전환하는 기업들

### 패스워드 기반 인증이 생산성 저해…

*조사에 따르면 63%가 패스워드를 잊어버려 중요 정보에 접근하는데 어려움을 겪은 경험을 갖고 있다.*




* By HYPR, 2022 State of Passwordless Security Report

**단점**

- 복잡한 문자열 요구
- 패스워드 유출, 분실
- 패스워드의 소유화
- 과거 패스워드 재사용

### 비밀번호 없는 생체정보 활용한 패스키

fido ALLIANCE simpler stronger authentication

*애플·구글·MS 패스워드 필요 없는 로그인 가속화 위해 FIDO 표준 지원 확대*

금융감독원 은행권 '생체인증'의무화…

제목 : 금융보안원 「금융권 생체정보 인증·관리 안내서」 발간
- 금융권의 안전한 생체인증 적용을 위해 필요한 보안대책 안내 -

* 03.2023 금융보안원 보도자료

**장점**

- 분실/유출 방지
- 저장/관리 문제 해결
- 생성의 불편 해소
- 강력한 신원 확인

21년도 기업 조직의 **89%**가 피싱 공격을 경험

# ZTNA 인증(2/2)

## FIDO 인증 표준의 패스키 지원으로 강력한 사용자 인증 및 식별

### 다중 인증(MFA)

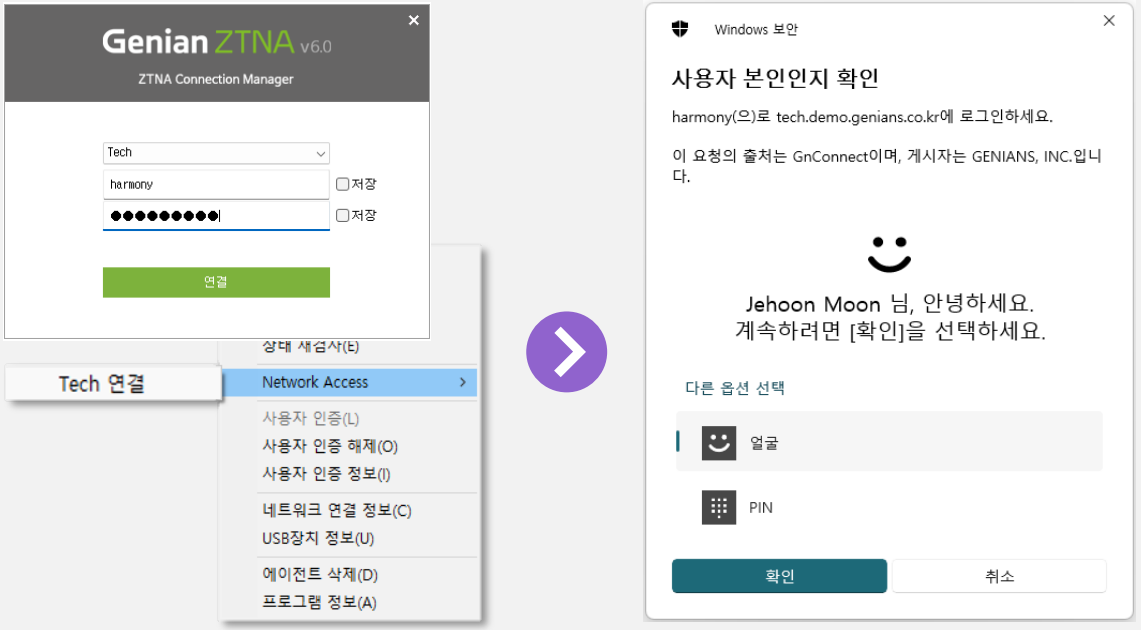
윈도우 Hello 및 애플 패스키 지원

PIN　Touch_ID　Face_ID

SMS　구글OTP　WebHook

Genian ZTNA 가 제공하는 다중 인증(MFA)

### 패스키 활용 사례




1차 비밀번호 인증

2차 패스키 인증

# ZTNA 가시성(1/4)

## 내/외부의 모든 단말기 정보 수집 및 분류, IP 실명 확인


| NT AG SS | 동작 | 가동률 | IP주소 | MAC주소 | NIC벤더 | 제어정책 | 인증사용자 | 부서명 | 호스트명(이름) | 등록시각 | 마지막 동작시각 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 82% | 10.11 | 2C:0D:A7:B6:F4:E5 | Intel Corporate | Agent Not Installed | 김 | 기술부/기술2팀 | BOOK-IHARSPMCFG | 2022-10-08 06:39··· | |
| | | 76% | 10.11 | F8:E4:3B:09:0A:21 | ASIX Electronics Cor··· | Agent Not Installed | 윤 | 기술지원센터/TAC2팀 | YOON | 2023-03-09 14:36··· | |
| | | | | 0C:9A:3C:E6:6A:B8 | Intel Corporate | Agent Not Installed | | | DESKTOP-N26SSJ7 | 2023-02-20 14:15··· | 2023-03-17 00:23··· |
| | | | | 3C:A6:F6:76:19:DB | Apple, Inc. | Agent Not Installed | | 술연구소/Endpo··· | 3c:a6:f6:76:19:db | 2023-03-06 14:51··· | 2023-03-27 08:34··· |
| | | 0% | 10.11 | A0:78:17:7F:B7:50 | Apple, Inc. | Agent Not Installed | 최 | 기술지원센터/TAC2팀 | MACBOOK-PRO | 2023-03-09 14:10··· | 2023-03-13 08:47··· |
| | | 0% | 10.11 | 00:E0:4C:68:00:3B | REALTEK SEMICOND··· | User Not Authentica··· | | | yckimui-MacBook··· | 2023-03-16 08:43··· | 2023-03-16 05:00··· |
| | | 96% | 10.11 | A0:78:17:6D:3E:2B | Apple, Inc. | Default Policy | 유 | 기술지원센터/TAC1팀 | dgryu-macbookpr··· | 2022-11-24 15:05··· | |
| | | 67% | | :65:8F:10 | Intel Corporate | Default Policy | 조 | | SKTOP-P3D8IAU | 2023-02-24 16:07··· | |
| | | 0% | 10.11 | 02:27:02:02:0A:70 | Unknown | Blocking Exceptions | 윤 | 기술지원센터/TAC2팀 | YOON | 2023-02-27 14:26··· | 2023-02-28 00:51··· |
| | | 57% | 10.11 | 04:EA:56:3E:16:AB | Intel Corporate | Default Policy | 문 | 컨설팅부/컨설팅2팀 | GGMSOON2 | 2022-12-26 14:04··· | |
| | | 44% | 10.11 | 0C:D2:92:F8:4F:D5 | Intel Corporate | Default Policy | 박 | 지니언스(주)/인프··· | 0c:d2:92:f8:4f:d5 | 2023-02-07 12:30··· | |
| | | 99% | 10.11 | 50:ED:3C:1F:6D:FB | Apple, Inc. | Block Exceptions (as··· | 이 | 지니언스(주)/인프··· | jws-MacBook-Air.l··· | 2022-12-20 12:13··· | |
| | | 57% | 10.11 | F8:E4:3B:0F:7F:D8 | ASIX Electronics Cor··· | Default Policy | 조 | 기술부/기술1팀 | f8:e4:3b:0f:7f:d8 | 2023-01-11 17:24··· | |
| | | 80% | 10.11 | 88:E9:F | | Default Policy | 이 | 엔드포인트보안연구··· | mouereui-Ma | | |
| | | 0% | 10.11 | E8:84:A5:2F:CF:06 | Intel Corporate | Blocking Exceptions | 앙 | 기술지원센터/TAC1팀 | SEONMIN-TEST | 2023-03-22 14:45··· | 2023-03-23 05:00··· |
| | | 96% | 10.11 | 5C:E9:1E:B5:22:27 | Apple, Inc. | Default Policy | 김 | 기술연구소/UX팀 | yckimui-MacBook··· | 2023-03-15 10:38··· | |
| | | 65% | 10.11 | 8C:B8:7E:60:0F:B8 | Intel Corporate | Default Policy | 유 | 엔드포인트보안연구··· | L3IADK-C2 | 2022-10-07 09:57··· | |
| | | 0% | 10.11 | E0:D5:5E:59:BC:3C | GIGA-BYTE TECHNO··· | Blocking Exceptions | 김 | 기술연구소/PM팀 | OLYMPUS2 | 2023-02-14 21:06··· | 2023-03-27 07:19··· |
| | | 0% | 10.11 | 70:A8:D3:13:2B:21 | Intel Corporate | | 권 | 기술부/기술1팀 | 권한준 | 2022-12-13 10: | |
| | | 79% | 10.11 | A0:78:17:69:B1:B1 | Apple, Inc. | Default Policy | 이 | 기술연구소/UX팀 | leejsui-MacBookPr··· | 2023-02-14 10:59··· | |
| | | 55% | 10.11 | A0:CE:C8:C1:E0:3E | CE LINK LIMITED | Default Policy | 박 | 지니언스(주)/인프··· | a0:ce:c8:c1:e0:3e | 2023-03-02 11:06··· | |
| | | 79% | 10.11 | E4:5E:37:A8:72:F8 | Intel Corporate | Default Policy | 김 | 엔드포인트보안연구··· | LAPTOP-N8J49673 | 2022-08-29 13:52··· | |

# ZTNA 가시성(2/4)

## 내/외부 단말의 다양한 가시성 제공

### 기본 정보

| | | | |
|---|---|---|---|
| | 10.64.0.2 DHCP | MAC 주소 | 00:E0:4C:68:00:17 |
| IPv6 주소 | | IPv6 링크로컬 | |
| 동작상태 | DOWN | 연결방식 | 가상 |
| 관리센서 | S-10.64.0.1 | 장비 | 10.64.0.2 (2/3) |
| 스위치(포트) | 10.64.0.1 (0) | 접속AP | |
| NATed IP | 43.200.194.48/37480 | NAT 장비 | 지정 |
| 최초 등록 | 2023-03-27 09:41:47 | 가동률 | 63.00% |
| 마지막 동작시각 | 2023-03-27 09:51:02 | 최근 노드 검사 | 2023-03-27 09:41:47 |
| 호스트명 | DESKTOP-ECVRIJ7 | DNS 이름 | |

| NT AG SS | 동작 | IP주소 | MAC주소 | 인증사용자 |
|---|---|---|---|---|
| | | 10.64.0.2 | 00:E0:4C:68:00:17 | 0 |
| | | 172.30.10.159 | 00:E0:4C:68:00:17 | 0 |
| | | 192.168.0.45 | 8C:17:59:B7:D3:AB | |

### HW 정보

| 제조사 | CPU 명 | CPU 제조사 | 리비전 | 배터리 | 온도 | CPU 사용량 |
|---|---|---|---|---|---|---|
| LG Electronics | 12th Gen Intel(R) Core(TM) i7-1260P | Intel Corporation | 591523 | 존재함 | | 1.88% |

메모리 정보

| 메모리 전체 | 사용 | % 사용 |
|---|---|---|
| 15.72 GB | 9.99 GB | 63.53% |

저장장치 정보

| 장치명 | 유형 | 벤더명/모델명 | 고유번호 | 볼륨ID | 파일시스템 | 총 용량 | 사용된 용량 | % 사용 |
|---|---|---|---|---|---|---|---|---|
| C: | 고정드라이브 | / SOLIDIGM SSDPFKNU010TZ | 0000_0000_0100_0000_B7D6_C8AB_1C01_0001. | 4E41-D532 | NTFS | 466.78 GB | 68.58 GB | 14.69% |
| D: (새 볼륨) | 고정드라이브 | / SOLIDIGM SSDPFKNU010TZ | 0000_0000_0100_0000_B7D6_C8AB_1C01_0001. | 36AF-D8A0 | NTFS | 466.63 GB | 97.86 GB | 20.97% |

운영체제 정보

| 운영체제 명 | 버전 | 빌드 버전 | 서비스팩 | IE 버전 | 언어 | 타임존 | 사용자 | 조직 |
|---|---|---|---|---|---|---|---|---|
| Microsoft Windows 11 Home x64 | 22H2 | 10.0.22621 | | 11.1.22621.0 | Korean | (GMT+09:00) Seoul, Tokyo | 관리자 | |

### SW 정보

| 제품 버전 | 현재패턴 버전명 | 현재패턴 날짜 | 실시간감시 | 최근검사시간 |
|---|---|---|---|---|
| 4.18.2201.11 | 1.385.1197.0 | 2023-03-27 00:55 | 동작 | 2023-03-22 11:44 |

소프트웨어목록

| 프로그램명 | 버전 | 경로 |
|---|---|---|
| AnySign4PC 1.1.2.0 | 1.1.2.0 | |
| AsyncTextService | 10.0.22621.1 | C:\Windows\SystemApps\Microsoft.AsyncTextService_8wekyb3d8bbwe |
| AudioDirector for LGE | 7.0.9105.0 | C:\Program Files\WindowsApps\www.cyberlink.com.AudioDirectorforLGE_7.0.9105.0_x64__srrv |
| Canon Office Printer Utility | 12.7.0.0 | C:\Program Files\WindowsApps\34791E63.CanonOfficePrinterUtility_12.7.0.0_x64__6e5tt8cgb93 |
| CapturePicker | 10.0.19580.1000 | C:\Windows\SystemApps\Microsoft.Windows.CapturePicker_cw5n1h2txyewy |
| Chrome | 111.0.5563.111 | C:\Program Files\Google\Chrome\Application |
| Clipchamp | 2.5.15.0 | C:\Program Files\WindowsApps\Clipchamp.Clipchamp_2.5.15.0_neutral__yxz26nhyzhsrt |
| ColorDirector for LGE | 5.0.8107.0 | C:\Program Files\WindowsApps\www.cyberlink.com.ColorDirectorforLGE_5.0.8107.0_x64__srrw |
| Cortana | 4.2204.13303.0 | C:\Program Files\WindowsApps\Microsoft.549981C3F5F10_4.2204.13303.0_x64__8wekyb3d8bbv |
| DTS:X Ultra | 1.11.11.0 | C:\Program Files\WindowsApps\DTSInc.DTSXUltra_1.11.11.0_x64__t5j2fzbtdg37r |

### 업데이트 정보

| | 분류 | 릴리즈 | 업데이트 상태 | 설치승인상태 | 업데이트시각 |
|---|---|---|---|---|---|
| 2023-03 x64 기반 시스템용 Windows 11 Version 22H2에 대한 누적 업데이트(KB5023706) | 보안 업데이트 | 2023-03-15 | 완료 | 설치미승인 | 2023-03-16 11:25:08 |
| Windows 악성 소프트웨어 제거 도구 x64 - v5.111(KB890830) | 업데이트 롤업 | 2023-03-15 | 완료 | 설치미승인 | 2023-03-16 17:14:40 |
| 2023-02 Windows 11, version 22H2 x64에 대한 .NET Framework 3.5 및 4.8.1 누적 업데이트(KB5022497) | 보안 업데이트 | 2023-02-15 | 완료 | 설치미승인 | 2023-03-16 17:14:40 |
| 2022-08 x64 기반 시스템용 Windows 11 22H2 보안 업데이트(KB5012170) | 보안 업데이트 | 2022-08-10 | 완료 | 설치미승인 | 2023-03-16 17:14:40 |
| LG - Monitor, Other hardware - LG FULLHD(HDMI) | | | 미완료 | 설치미승인 | 2023-03-16 11:25:08 |
| 2023-01 Update for Windows 11 Version 22H2 for x64-based Systems (KB4023057) | | | 완료 | 설치미승인 | 2023-03-16 11:25:08 |
| Update for Windows Defender Antivirus antimalware platform | | | 완료 | 설치미승인 | 2023-03-16 17:14:40 |

# ZTNA 가시성(3/4)

## 트래픽 및 어플리케이션의 가시성 제공

| 시간 | 출발지 | 출발지 P… | 목적지 | AS 조직명 | 목적지 P… | 서비스 | Applicatio… | 호스트명 | 프로토… | Packets | Bytes | 사용자 | 장비명 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2023-02-22 13:07:18 | 10.64.1.137 | 58043 | 172.217.25.163 | GOOGLE | 80 | http | Google | www.gstatic.com | tcp | 96 | 4.25 KB | leedh13 | S-10.64.1.1 |
| 2023-02-22 13:07:18 | 10.64.1.137 | 58005 | 142.250.76.133 | GOOGLE | 443 | https | GMail | mail.google.com | tcp | 142 | 28.49 KB | leedh13 | S-10.64.1.1 |
| 2023-02-22 13:07:… | 10.64.1.137 | 58110 | 52.22.149.1 | AMAZON-… | 443 | https | Amazon… | …er.customercase.com | tcp | 82 | 14.46 KB | leedh13 | S-10.64.1.1 |
| 2023-02-22 13:07:14 | 10.64.1.137 | 58101 | 3.34.224.161 | AMAZON-02 | 443 | https | TLS | tech.demo.genians.co… | tcp | … | 20.03 KB | leedh13 | S-10.64.1.1 |
| 2023-02-22 13:05:18 | 10.64.1.137 | 58107 | 172.31.194.14 | | 443 | https | | | tcp | 4 | 208 B | leedh13 | S-10.64.1.1 |
| 2023-02-22 13:05:13 | 10.64.1.137 | 61712 | 172.217.25.170 | GOOGLE | 443 | https | | | udp | 138 | 18.62 KB | … | S-10.64.1.1 |
| 2023-02-22 13:05:13 | 10.64.1.137 | 54784 | 8.8.8.8 | GOOGLE | 53 | domain | Google | | udp | 4 | 338 B | leedh13 | S-10.64.1.1 |

1 누가
2 언제
3 어떤 IP로
4 어느 지역 어디와
5 어떤 서비스 채널을 통해
6 어떤 어플리케이션을
7 얼마나 통신하였는가

### 분석

네트워크 및 어플리케이션
사용 행위 분석

### 통계

부서, 사용자, 장비

- 어플리케이션 사용 List
- 목적지(DST)별 사용 List

### 활용

정책 및 모니터링 활용

- 정책 데이터 활용
- 특정 이벤트 발생시 제어 or 알람
- 비정상 트래픽 감시

# ZTNA 가시성(4/4)

## 클라우드에 동작 중인 인스턴스에 대한 가시성 제공

Cloud 인스턴스 리스트 수집

| NT AG SS | 동작 | IP주소 | MAC주소 |
|---|---|---|---|
| | | 10.1.124.22 | 26:A0:09:2F:D7:A5 |
| | | 192.168.0.126 | 02:EB:DE:0F:42:66 |
| | | 192.168.2.213 | 02:F2:BF:47:C4:E2 |
| | | 192.168.7.54 | 02:D9:1D:D0:5F:28 |
| | | 192.168.7.104 | 02:AD:D0:6E:EB:24 |
| | | 192.168.11.3 | 02:39:B9:31:FF:3A |
| | | 192.168.38.217 | 02:90:97:8F:45:C6 |

Cloud 인스턴스 상세 정보 JSON

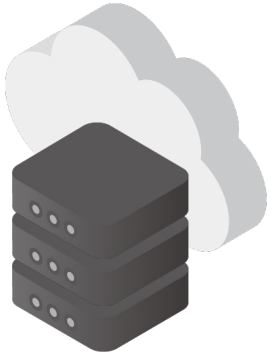

```
aws.Address.Domain: "vpc"
aws.Address.PublicIp: "43.201.174.138"
aws.Address.CarrierIp:
aws.Address.InstanceId: "i-01ab401d64b139b3c"
aws.Address.AllocationId: "eipalloc-05c6b91fb0c249409"
aws.Address.AssociationId: "eipassoc-09e58d4b775a2a60f"
aws.Address.PublicIpv4Pool: "amazon"
aws.Address.CustomerOwnedIp:
aws.Address.PrivateIpAddress: "192.168.2.213"
```


Cloud 인스턴스 상세 정보 JSON

CLOUD TYPE

Cloud 정보 / 같으면 (Object/Value)

| 2 | 1 | 2 |
|---|---|---|
| cloud T2micro | cloud T2medium | cloud T2large |



### 통합 관리

내부 망 뿐만 아니라 Cloud에 이르기 까지
가시성 제공 및 통합 관리가 가능합니다.

### 변화 감지

관리자의 승인없이 생성되거나 동작하는
인스턴스들에 대한 모니터링 및 가시성을
제공합니다.

### 멀티 Cloud 지원

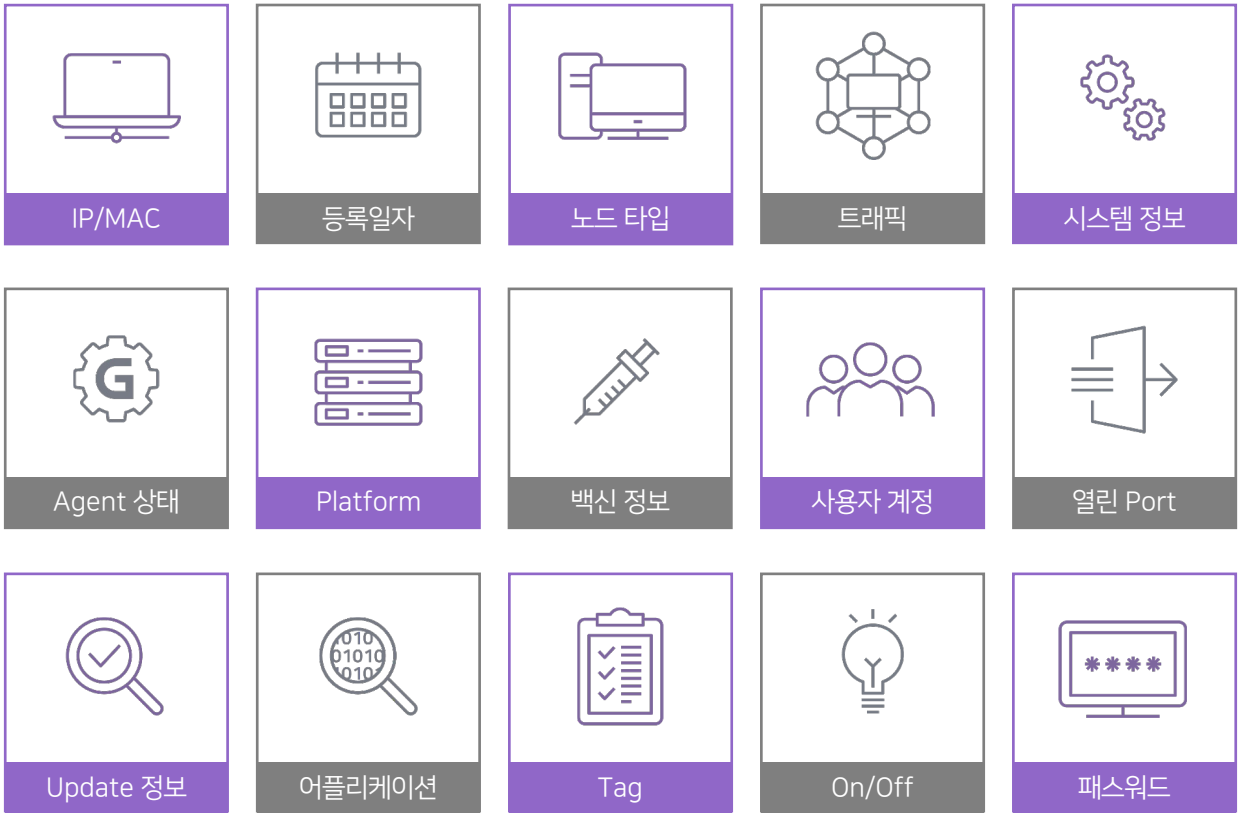
aws

NAVER Cloud

# ZTNA 분류(1/2)

## 다양한 Context를 활용한 통제 정책 수립

사용자 및 부서, 단말상태 등 약 600여가지 이상의 조합을 이용한 그룹화




**그룹 조건**

- 플랫폼 / 감지된 플랫폼이 같으면 / **Microsoft Windows**
- 업/다운상태 / 상태값 / **UP**
- IP 관리 / IP정책 / **차단됨**
- USB 장치 정보 / 특정 클래스가 존재하면 / **WebCam**
- 장비내 무선랜 / 무선랜그룹에 속하는 AP가 존재하면 / **Corporate SSIDs**

- 노드 타입 / 감지된 노드타입이 같으면 / **PC**
- 업/다운상태 / 상태값 / **UP**
- 인증 사용자 / 인증상태 / **인증되지 않음**
- 백신 정보 / 존재여부 / **존재안함**
- 백신 정보 / 패턴날짜가 보다 오래되면 / **1 주, 백신명=모든 백신**

- 시스템 사용자 계정 / 비밀번호없는 로그인된 계정 존재 /
- 계정 비밀번호 검증 / 취약이 존재하면 /
- 시스템 / 방화벽 / **사용안함**
- 에이전트 상태 / 설치상태 / **설치안됨**
- 시스템 / 배터리 / **존재함**

- 등록 일자 / 특정시간 이내에 등록된 / **1 개월**
- 태그 / 존재하면 / **GUEST**
- 열린 포트 / 지정 포트가 존재하면 / **TCP, Port: 443**
- 서약 동의 / 노드가 서약동의하지 않은 / **보안서약동의**
- 시스템 / 공유폴더 / **쓰기허용**

- 트래픽 / (TCP/전체)가 보다크면 / **800 MB/s**
- 노드 그룹 / 속하면 / **PC**
- IP 관리 / 충돌보호 / **위반됨**
- NAT / NAT상태가 같으면 / **NAT 서비스제공 장치**

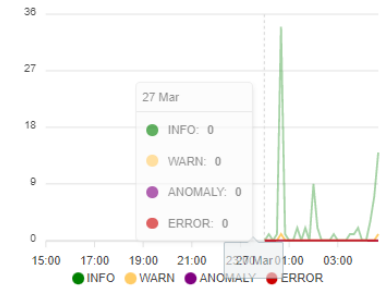
# ZTNA 분류(2/2)

## 대시보드를 통한 통계 및 현황 제공

- 분류(SW, HW, Flow 등)별 위젯 제공
- 관리자에 맞는 커스텀 위젯 구성 가능
- PDF, PPTX, DOCS export 제공

### 감사로그 현황

감사로그 타임차트




### 서비스 분류

서비스 현황

| | |
|---|---|
| DHCP 서버 | |
| DNS 서버 | 1 |
| FTP서버 | 0 |
| Secure 웹서버 | 0 |
| SMB공유 | 0 |
| SMTP서버 | 0 |
| SNMP 서버 | 0 |
| TELNET 서버 | 0 |
| 웹서버 | 0 |

### 플랫폼 분류

노드 플랫폼

| | | |
|---|---|---|
| Microsoft Windows 11 Home x64 | 6 | 38% |
| Ubuntu Linux 20.04 | 5 | 31% |
| Unknown | 2 | 13% |
| Intel Corporate | 1 | 6% |
| Linux | 1 | 6% |
| Microsoft Windows 10 Professional x64 | 1 | 6% |
| Vodavi XTS-IP PBX | 1 | 6% |

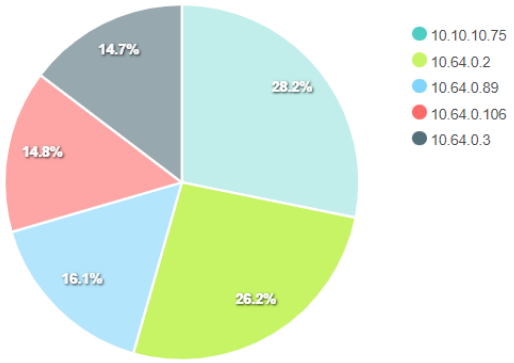
### 타입별 분류

노드 타입

| | | |
|---|---|---|
| PC | 7 | 35% |
| 서버 | 6 | 30% |
| IoT/OT/Etc | 4 | 20% |
| 센서 | 2 | 10% |
| Cloud 센서 | 1 | 5% |
| Agent센서 | 0 | 0% |
| 가상센서 | 0 | 0% |
| VOIP | 0 | 0% |
| 프린터 | 0 | 0% |
| 보안장비 | 0 | 0% |

### 트래픽 분류

FLOW SOURCE IP 트래픽 TOP PIE




FLOW SOURCE IP 트래픽 TOP

| Source IP | Bytes | Packets |
|---|---|---|
| 10.10.10.75 | 224.41 MB | 584,017 |
| 10.64.0.2 | 208.99 MB | 299,781 |
| 10.64.0.89 | 128 MB | 257,943 |
| 10.64.0.106 | 117.99 MB | 185,128 |

ZTNA CLIENT 사용자별 트래픽 TOP

| | | |
|---|---|---|
| leedh13@genians.com | 228.44 MB | 416,929 |
| cuyu9779 | 225.27 MB | 582,391 |
| marketer | 163.55 MB | 260,199 |
| Local Bridge | 35.32 MB | 183,788 |

# ZTNA 통제(1/2)

## 다양한 Context 를 활용한 실시간 동적 접근제어

### 다양하게 수집된 Context 정보를 활용한 Compliance 정책 수립

신규 IP&MAC

필수 소프트웨어 미 설치

윈도우 보안 패치 미 준수

미 인증 사용자

바이러스 감염 PC

위험 발생 여부

EOS OS 사용

불법소프트웨어 사용

공유 폴더 사용

실시간 검사

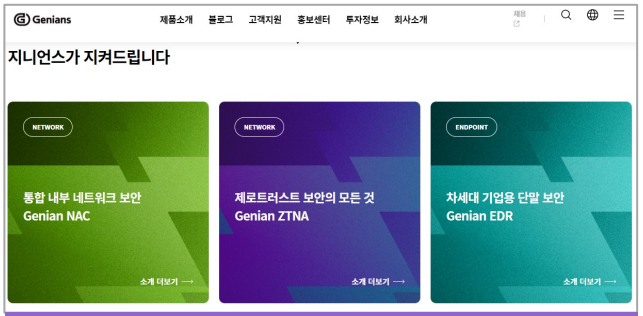
접근 통제

차단

허용

### 상태 변화에 따른 실시간 동적 접근권한 부여


차단 사유 및 교정 방안 안내




내부 서비스 접속

# ZTNA 통제(2/2)

## RBAC 기반에 최소 권한 부여

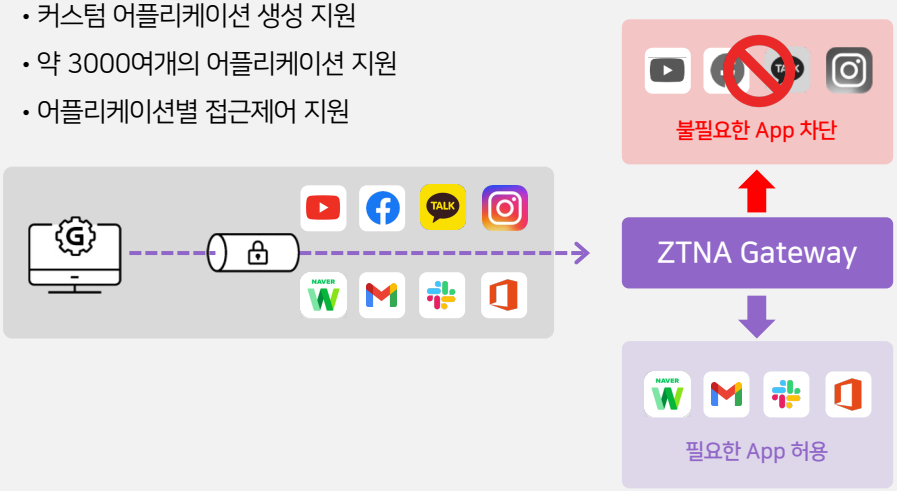
### 통제 조합

**더욱 세분화된 정책 제공(Microsegment)**

네트워크 그룹(목적지 IP) + 서비스(Port) + 시간 + 어플리케이션

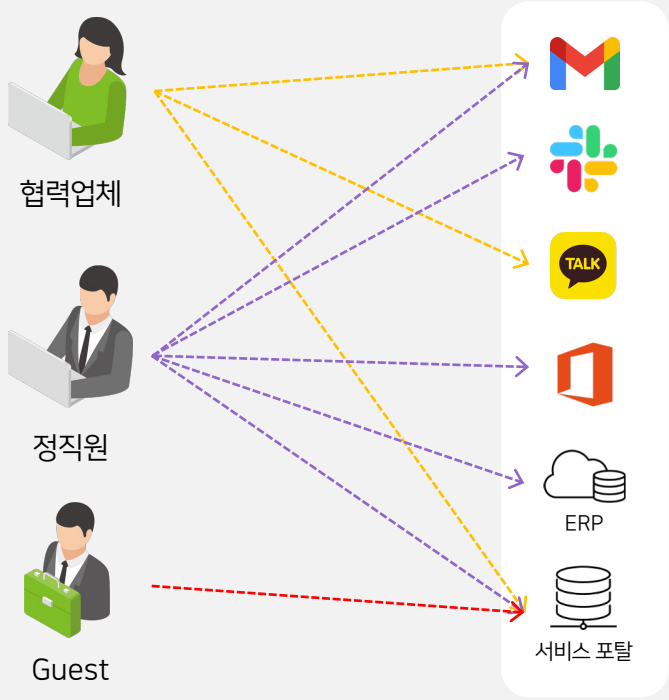
### 어플리케이션 제어

- 커스텀 어플리케이션 생성 지원
- 약 3000여개의 어플리케이션 지원
- 어플리케이션별 접근제어 지원




### 권한 중심의 통제 제어

**사용자 및 그룹별 권한에 따른 애플리케이션 선택적 제어**



# ZTNA 사용자 시나리오

## 사용자/장치의 위치와 상관없이 일관된 통제 정책 적용

### PC 무결성(Compliance) 검증

- PC내의 불법소프트웨어, 필수소프트웨어 사용 유무
- 회사내 컴플라이언스 정책 등 검증

### 사용자 인증

- 다중 인증(MFA)을 통한 강력한 사용자 인증
- 지문, 얼굴인식 등 생체정보를 통한 사용자 식별
- 정책 기반 사용자 접근 통제

### 장치 인증

- 사전 장비 인증을 통해 허가 단말 분류
- 인가 되지 않은 장치 접속 통제


### 안전한 연결

- 어느 곳(Anywhere), 언제나(Always) 항상 안전한 연결

### 접근 통제

- 출발지 사용자/장치 정책 세분화
- 1회성 허용이 아닌 실시간 동적 목적지 제어
- IP/TCP/UDP/PORT 외 어플리케이션 제어

### 최소 권한

- RBAC 기반 최소 권한 부여로 횡적 트래픽 제어
- 내부 위협 발생시 피해영역 최소화

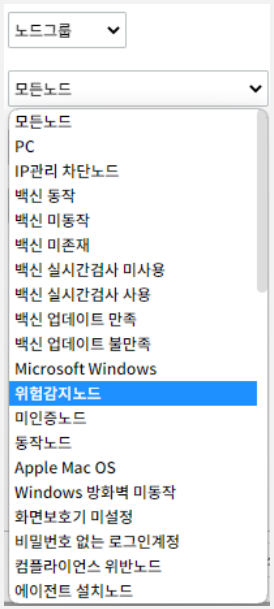
# ZTNA 특장점

## 보안그룹 관리 기능으로 클라우드 워크로드에 대한 동적 목적지 제어

- 클라우드에 분산된 보안그룹에 대해 자동화된 통합 관리 지원
- 클라우드 인스턴스 Security Group 과 노드 그룹의 IP목록 동기화 지원
- 클라우드 인스턴스 Level 의 통제 기능 제공

**정책 소스**

정책 소스 IP변경 시 자동 동기화





클라우드 보안그룹 정책 자동 적용

**클라우드 보안그룹 정책**

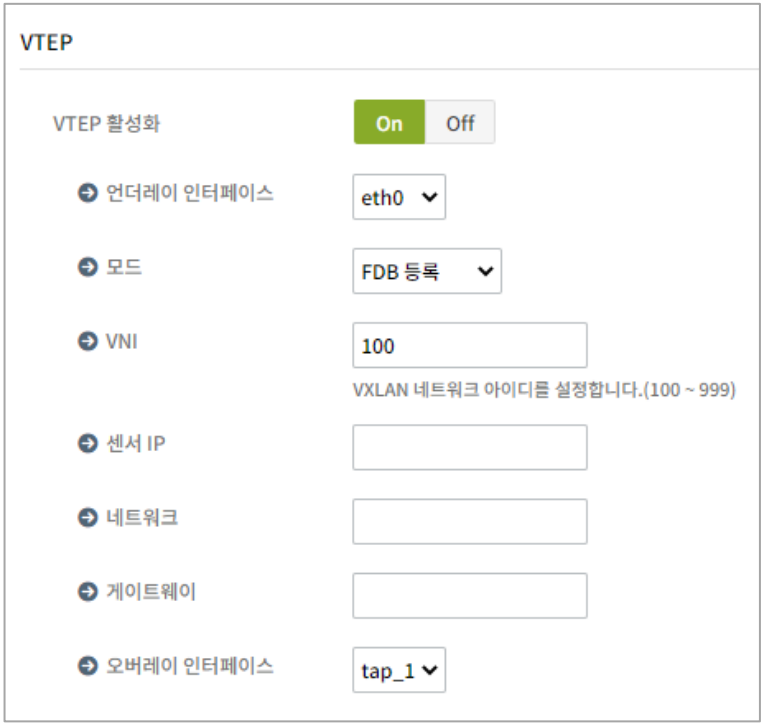
| TF | 이름 | 사이트 | Inbound | Outbound | Tags | 설명 |
|---|---|---|---|---|---|---|
| | agent_allow | TechZTNA | NET agent / TCP-ALL | IP 0.0.0.0/0 / ALL | Name = agent_allow | agent_allow |
| | dns_allow | TechZTNA | IP 0.0.0.0/0 / DNS | IP 0.0.0.0/0 / ALL | Name = dns_allow | dns_allow |
| | filebeat_outbound | TechZTNA | | NET policy / filebeat | Name = filebeat_allow_outbound | filebeat_outbound |
| | ssh_allow | TechZTNA | NET gateway / ssh | IP 0.0.0.0/0 / ALL | Name = ssh_allow | ssh allow |
| | web_allow | TechZTNA | IP 0.0.0.0/0 / TCP-WEB | IP 0.0.0.0/0 / ALL | Name = port_443_allow | port 443 allow policy |

# ZTNA 특장점

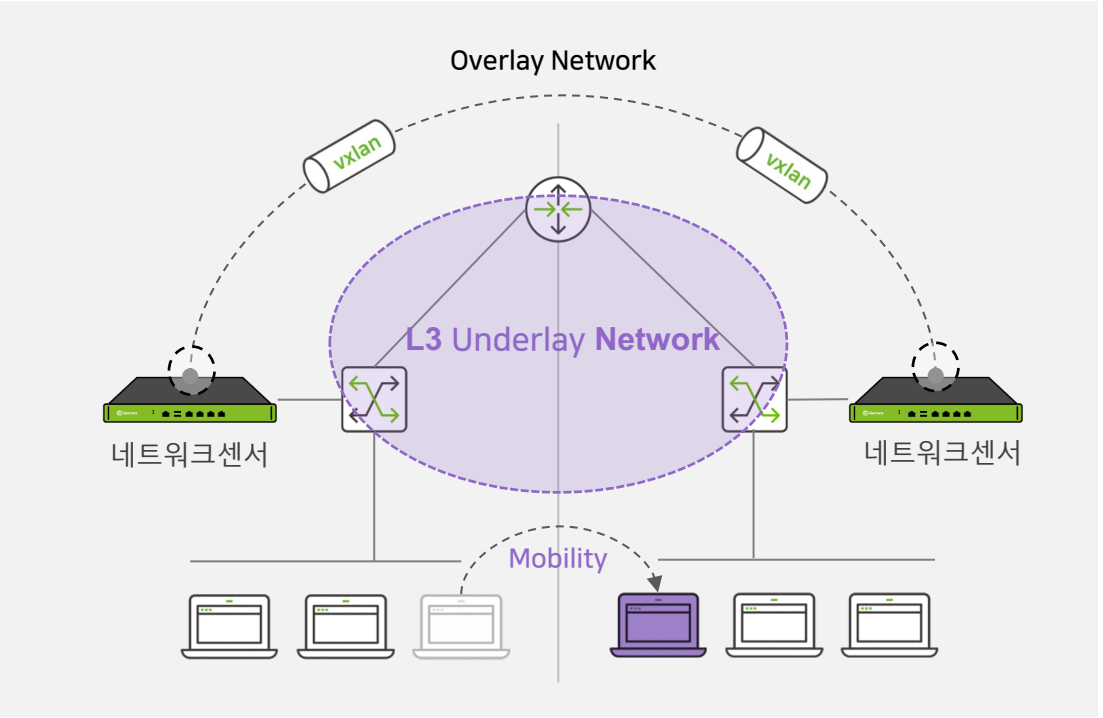
## IP-Mobility 지원으로 단말 이동 시에도 일관된 보안정책 적용

- 층간 이동에 따른 IP Mobility 제공
- 사용자 이동이 잦은 환경 적합

**확장 네트워크 설정** 네트워크 센서 VXLAN 설정 화면




**VXLAN 개념 구성도** 네트워크 인프라 보안정책 변경 불필요

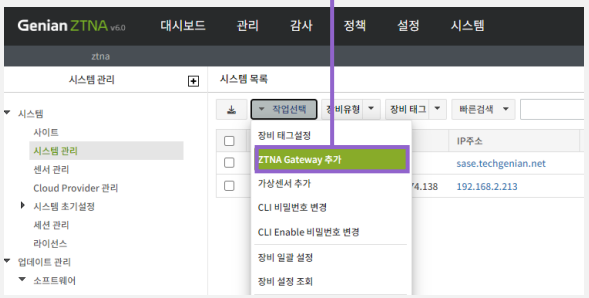


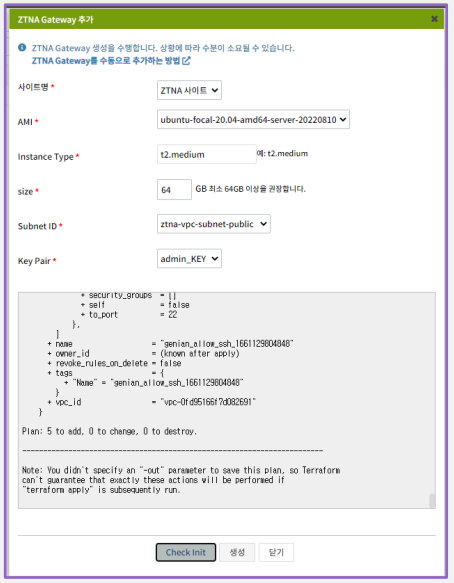
# ZTNA 특장점

## Terraform을 이용한 ZTNA Gateway 원 클릭 설치 지원

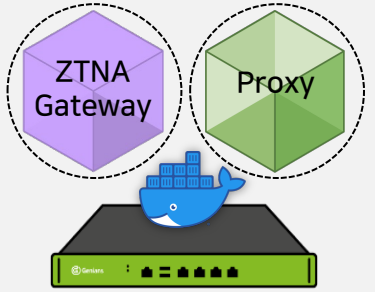
- 도커 컨테이너 지원으로 설치 간소화 및 서버 사용 환경에 따른 제약 최소화
- 컨테이너 이미지를 통해 빠르고 안정적인 배포 및 업그레이드 지원

HashiCorp Terraform




원 클릭으로 클라우드 환경에
ZTNA Gateway 생성

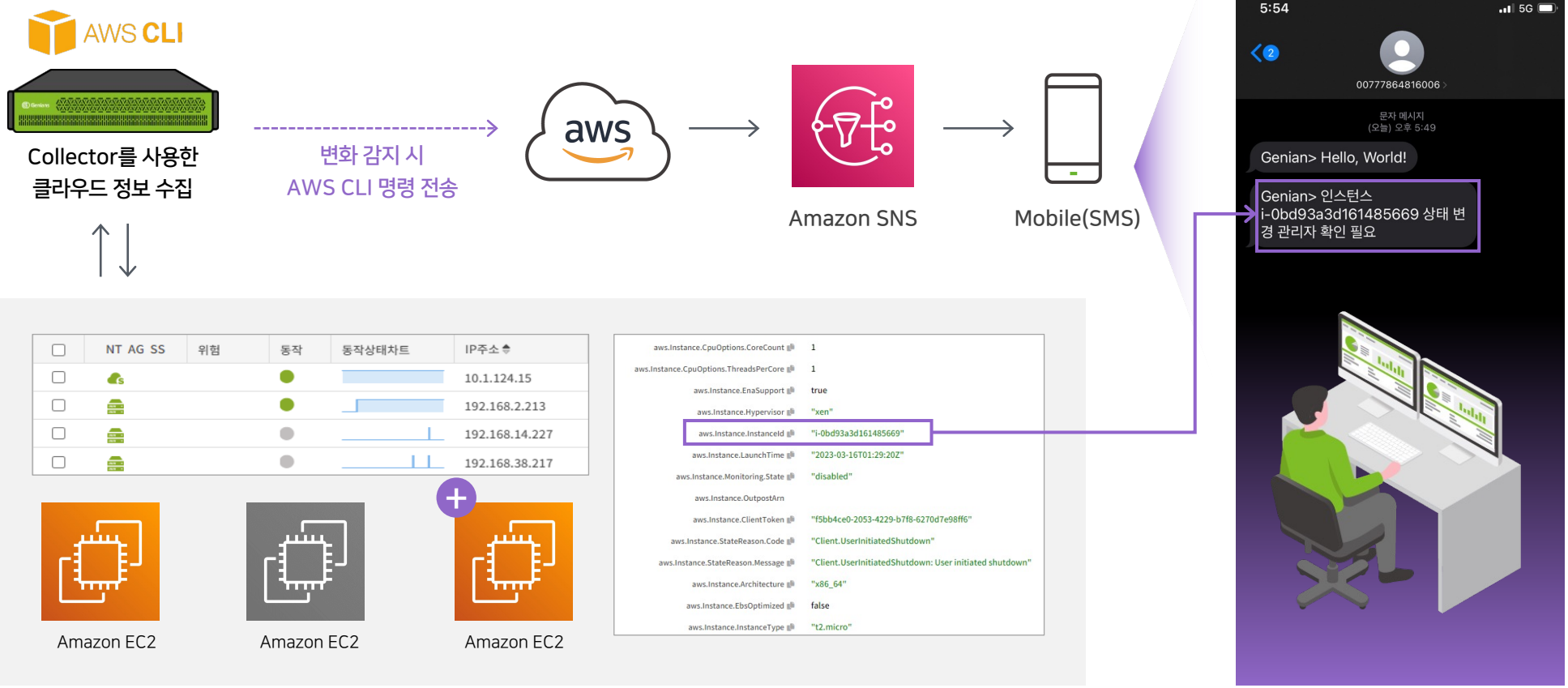

ZTNA Gateway

AMD64, ARM64 CPU
아키텍처 지원

# ZTNA 특장점

## AWS CLI 도구를 통한 AWS 서비스 관리 기능 제공

**활용사례)** 확인되지 않은 EC2 인스턴스 생성 및 상태 변경 시 Amazon SNS 서비스를 통한 관리자 SMS 전송

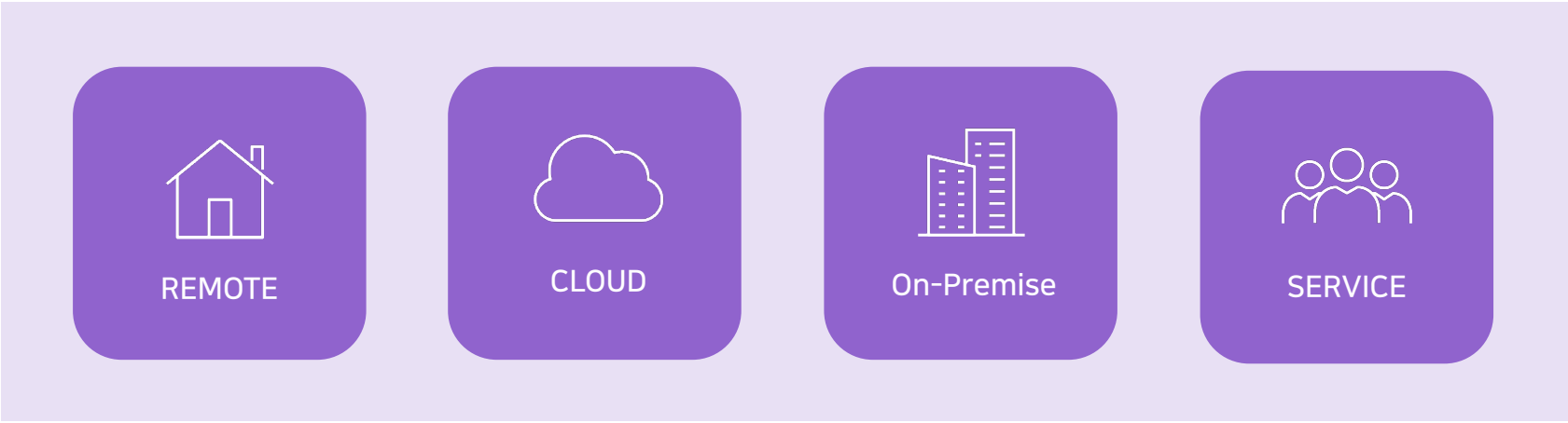


03

# Genian ZTNA 도입 효과

# ZTNA 도입효과

## 언제 어디서나 누수 없는 보안 정책 적용으로 Always on ZTNA를 실현합니다.




### 비용 감소

환경 변화에 따른 신규
보안시스템 도입 및 운영
인력 증가에 따른 비용 감소

### 운영 단순화

단일 솔루션으로 리모트 /
클라우드 / 온-프레미스
통합 관리 및 정책 지원

### 보안 에코시스템

자체 API 제공 및 클라우드
관리 도구와 다양한 Third
Party 솔루션과의 연동 지원

# ZTNA 도입효과

## 국가 단위에서 사이버 보안 모델로 채택된 ZTA(Zero Trust Architecture)

| 제로트러스트를 위한 7가지 원칙(NIST) | Genian ZTNA 해당 항목 |
|---|---|
| 1. 모든 데이터 및 컴퓨팅 서비스는 리소스로 간주 | 1-1. 네트워크에 연결된 모든 IT자산에 대한 자동 탐지 및 분류<br>1-2. 탐지된 모든 정보는 보안정책으로 수립되어 접근 통제 등에 활용 |
| 2. 모든 통신은 위치에 관계없이 보호 | 2. ZTNA Agent 와 Gateway 를 통한 양종단간 통신 암호화 지원 |
| 3. 리소스에 대한 접근은 세션별로 부여 | 3. 접속 단말의 컨텍스트에 따라 묶인 그룹별 최소 접근권한 할당 |
| 4. 리소스에 대한 접근은 다양한 상태에 따라 통제 | 4. 인증, 위치, 단말 보안 등 약 600가지 이상의 조합으로 생성한 그룹을 통한 접근통제 |
| 5. 모든 자산에 대한 무결성 및 보안상태에 대한 측정 | 5-1. 에이전트와 네트워크 자동 탐지를 통한 IT자산에 대한 보안 검증<br>5-2. 상태 정보 변경 시 그에 다른 다양한 제어 정책 적용(차단, 재 인증, 교정 등) |
| 6. 인증과 권한은 접근 이전에 동적이고 엄격하게 수행 | 6. 단말의 동적 컨텍스트 정보에 따라 유연한 접근통제 수행 (先 검증 後 접속) |
| 7. 가능한 많은 정보를 수집하고 보안 개선을 위해 활용 | 7. 수집된 IT자산 정보를 제공 할 수 있는 연계 기능 제공 |

* NIST SP 800-207 Zero Trust Architecture

Genian ZTNA는 제로트러스트를 위한 7가지 원칙을 충실히 지원하고 있습니다.

통합 보안 플랫폼 기업, 지니언스

# THANK YOU :)

Genians