

Genian Cloud ZTNA

지니언스(주)

Table of Contents

01. Cloud ZTNA 개요

02. Cloud ZTNA 제품 소개

03. Cloud ZTNA 활용 방안

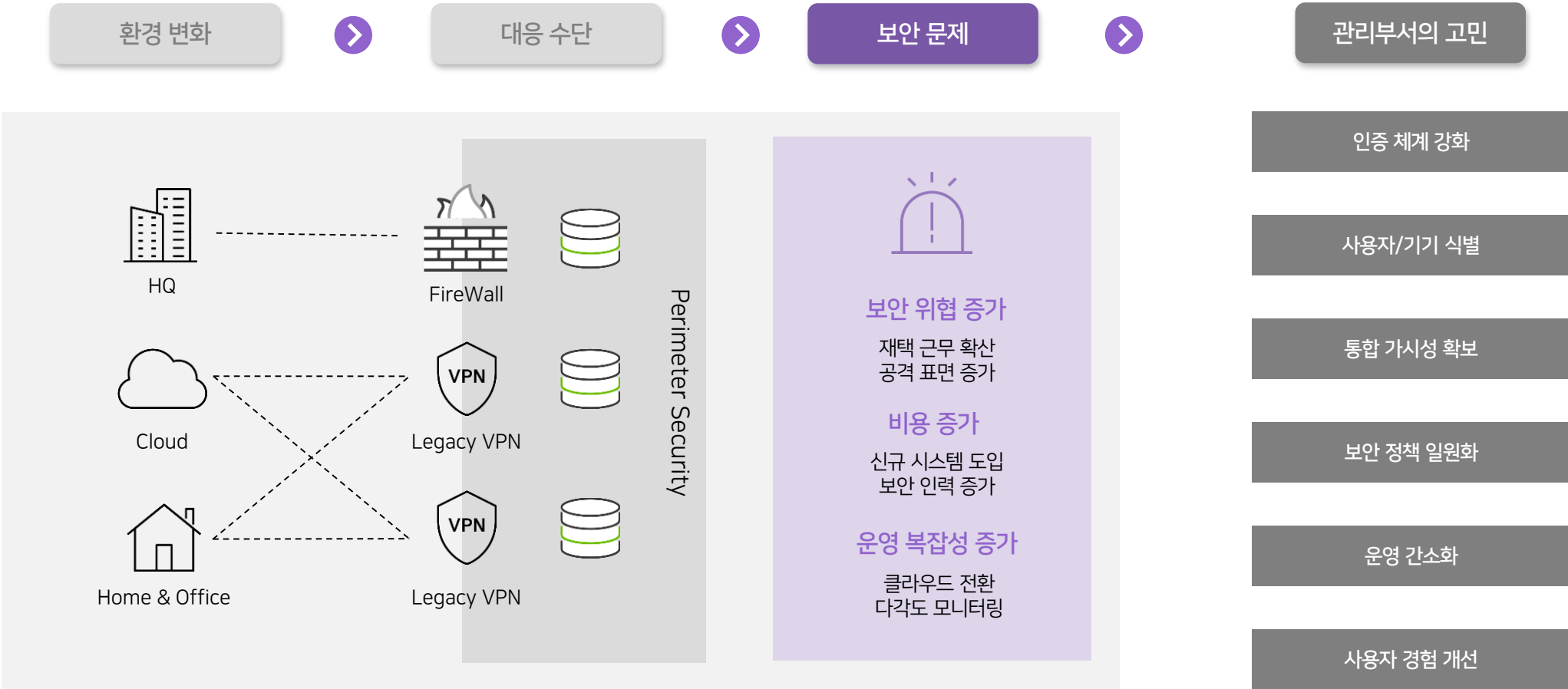
04. Summary

01.

Cloud ZTNA 개요

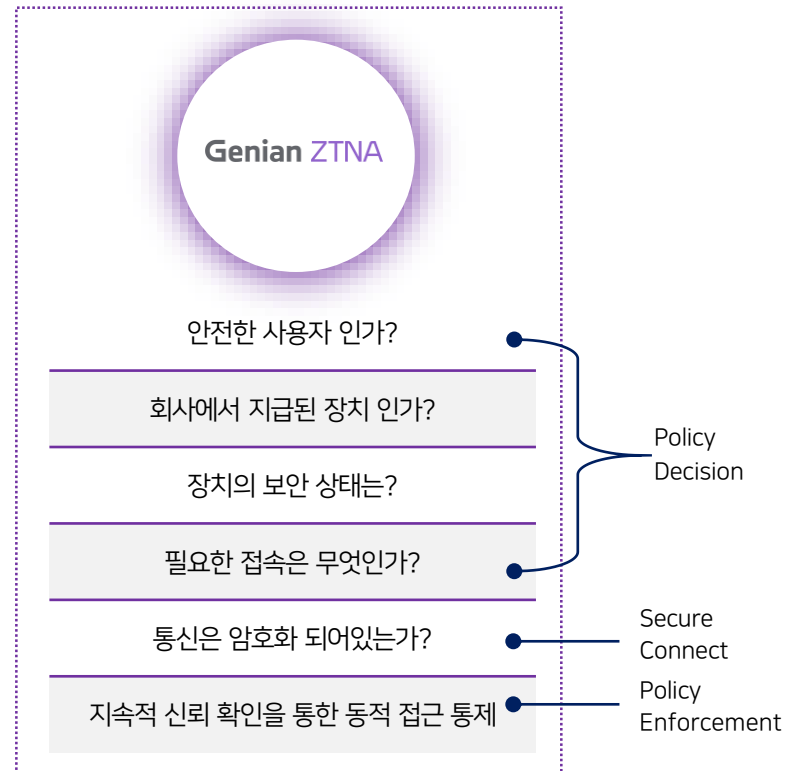
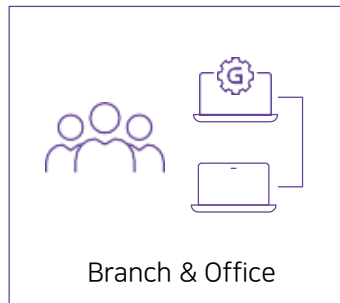
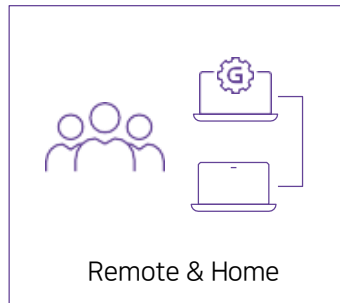
변화된 기업의 IT환경

- 통제 영역을 벗어난 새로운 업무 환경의 추가에 따른 보안 위협 및 고려사항 발생



- ZTNA(Zero Trust Network Access)는 사용자의 위치와 상관없이 인증되고 허용된 사용자만 필요한 서비스에 접근 허용

Remote & Branch Office



End Destination



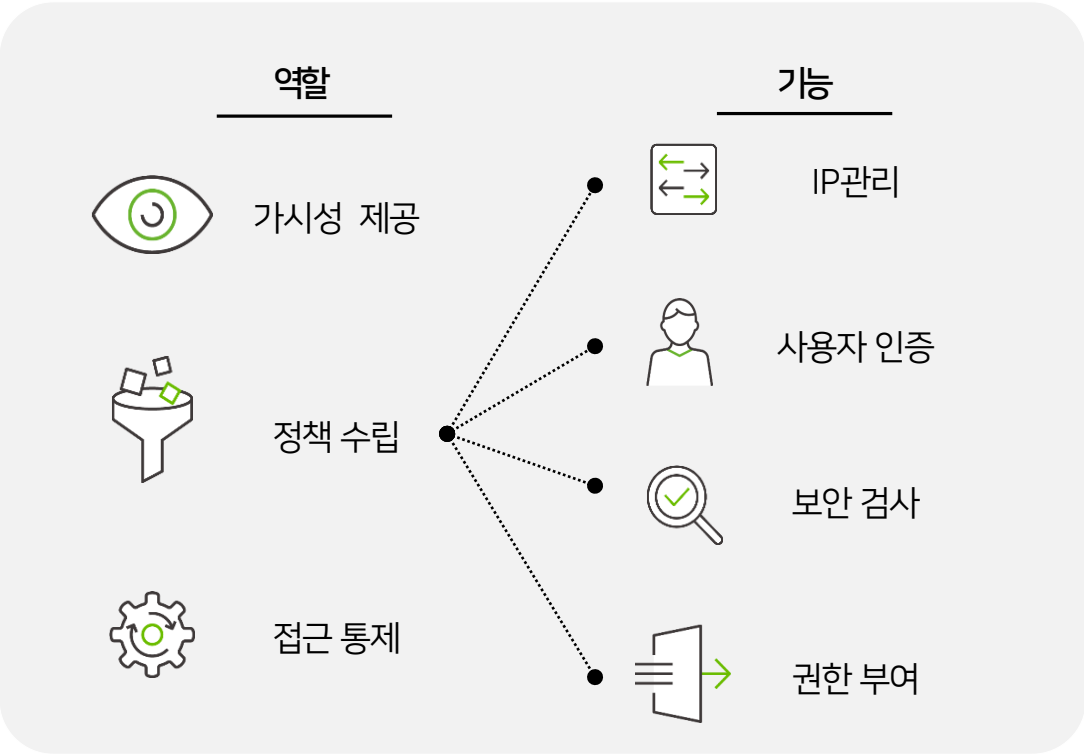
02.

Cloud ZTNA 제품 소개

NAC 보안의 한계점

NAC 기반의 네트워크 보안

NAC 는 기업 내부 네트워크에 사용자 및 기기를 식별하고 지속적인 보안 상태를 검증하여 리소스 및 서비스에 대한 접근을 허용하거나 차단



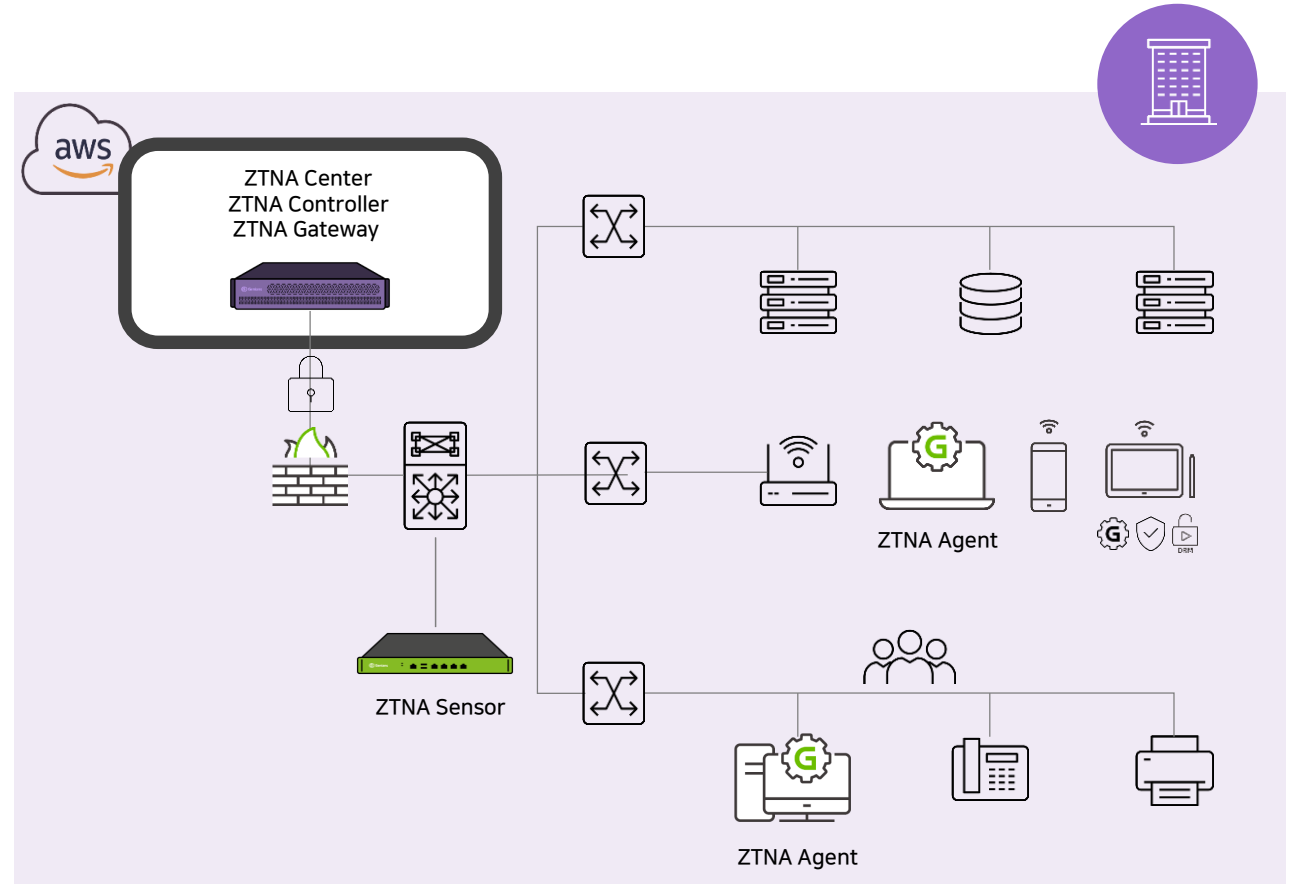
NAC 기반의 네트워크 보안 한계점

NAC 또한 전통적인 경계 기반의 보안 솔루션으로 기업의 변화된 IT환경을 지원하는데 있어 솔루션의 한계점 존재

제로 트러스트 원칙	NAC의 접근 방식	한계점
동적인 정책 적용	네트워크 접근 정책의 동적 적용 가능	클라우드, 원격 근무 등 변화하는 IT 환경에 대한 지원 부족
마이크로세그멘테이션	네트워크 세분화를 통해 일정 수준의 세그멘테이션 제공	네트워크 세분화에는 효과적이거나, 애플리케이션 또는 서비스 수준의 미세한 세그멘테이션에는 제한적
최소 권한 부여	네트워크 접근 제어를 통해 최소 권한 부여 정책 적용	네트워크 수준에서의 권한 부여에 제한되며, 애플리케이션 또는 데이터 수준에서의 세밀한 권한 조절에는 한계가 있음
지속적인 모니터링 및 검토	네트워크 활동의 모니터링과 분석을 제공	네트워크 활동에 집중하며, 사용자 행동이나 애플리케이션 수준에서의 지속적인 모니터링에는 한계

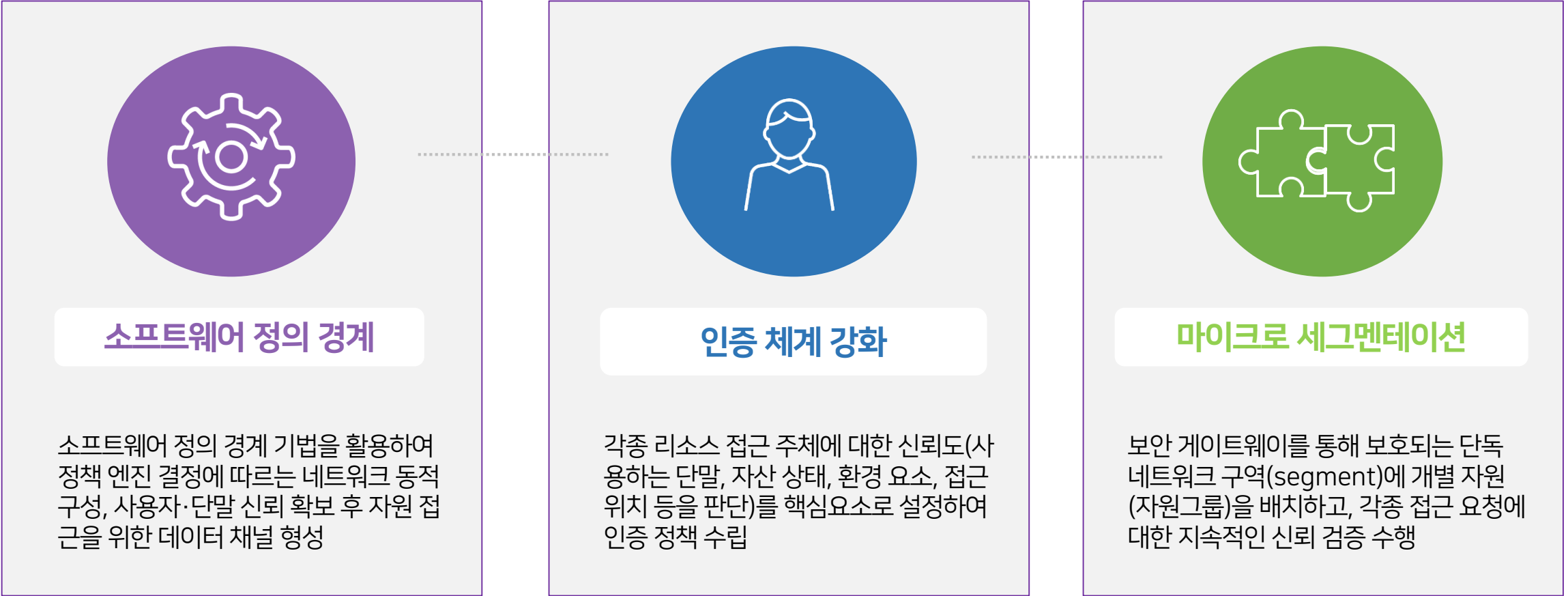
- NAC 기본 구성 외 확장 가능한 추가 구성 제공 및 온-프레임 / 클라우드 / 하이브리드 환경 구성 지원

ZTNA 구성요소	주요 기능	폼팩터(Form Factor)
ZTNA Center	<ul style="list-style-type: none"> · 내/외부 통합 정책 수립 및 관리 · 유/무선 네트워크 통합 관리 · 사용자 통합 인증 	
ZTNA Controller	<ul style="list-style-type: none"> · 사용자 및 기기 인증 · 사용자 서비스 간 연결 제어 	
ZTNA Gateway	<ul style="list-style-type: none"> · 보안 통신(SSL VPN) · 외부 네트워크 접근 통제 · 애플리케이션 인지 및 통제 등 	<ul style="list-style-type: none"> · 소프트웨어 · 일체형 Appliance · 가상화(VM)
ZTNA Sensor	<ul style="list-style-type: none"> · 내부 네트워크 가시성 제공 · 내부 네트워크 정보 수집 및 통제 	
ZTNA Agent	<ul style="list-style-type: none"> · 인증 클라이언트 · 단말 무결성 검사 · 단말 정보 수집 및 통제 지원 	<ul style="list-style-type: none"> · 소프트웨어



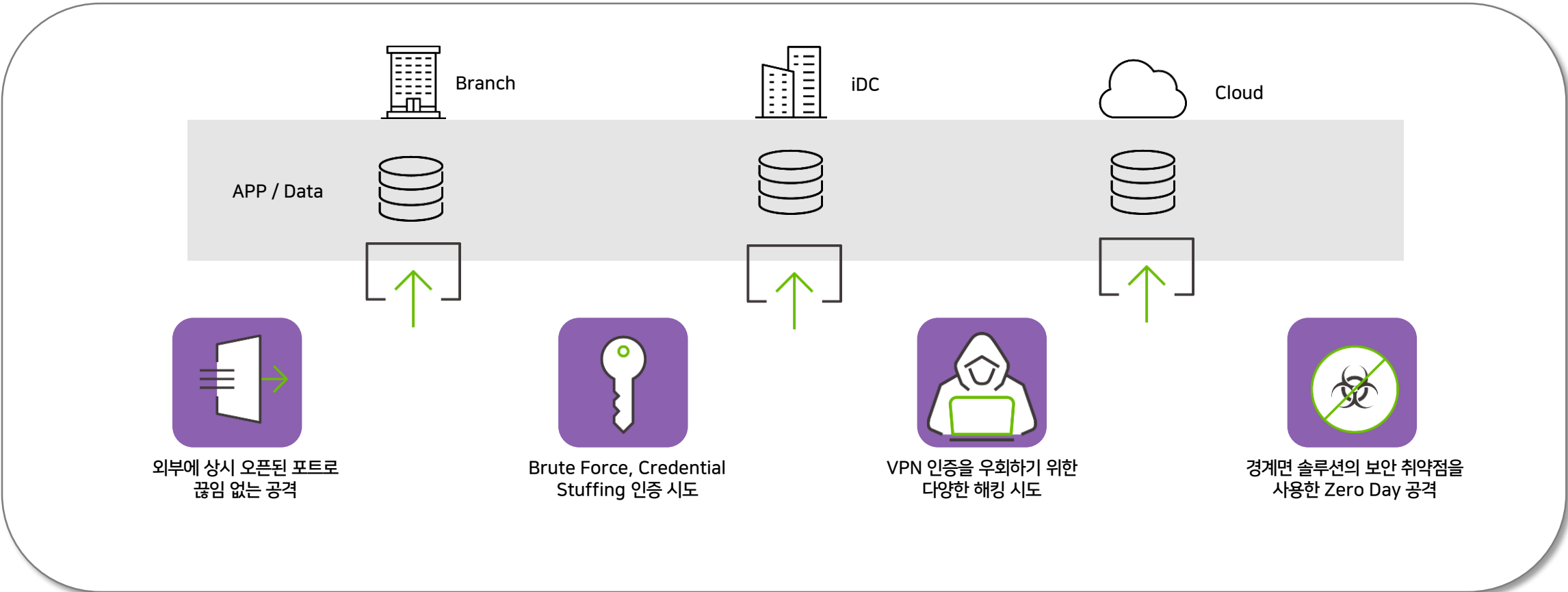
ZTNA가 제공하는 네트워크 접근 방식

- ZTNA 는 네트워크 접근 단계에 제로트러스트 핵심 원칙 3가지를 중점으로 신뢰할 수 있는 안전한 네트워크 액세스를 제공



소프트웨어 정의 경계 [네트워크 접근 전환의 필요성]

- 기존 전통적인 네트워크 접근 방식은 상시 오픈 되어 있는 서비스로 인해 공격 표면이 증가함과 동시에 소프트웨어의 취약점 등을 악용한 인증 우회 및 DDoS 공격 등에 취약함



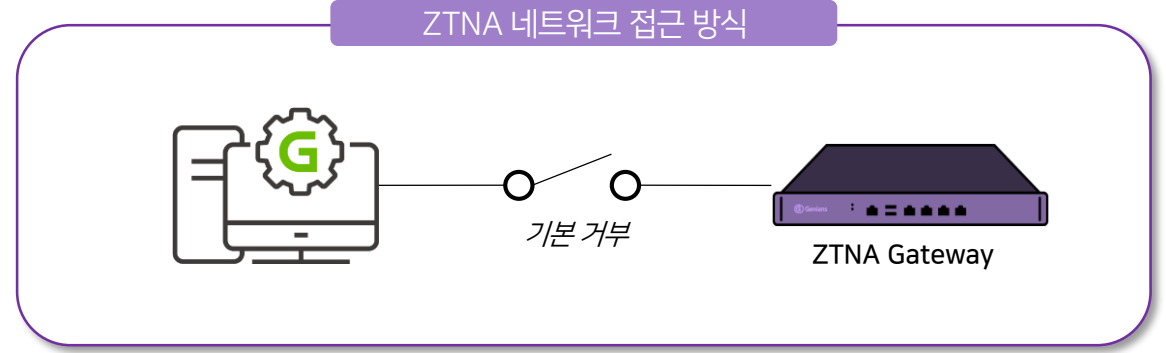
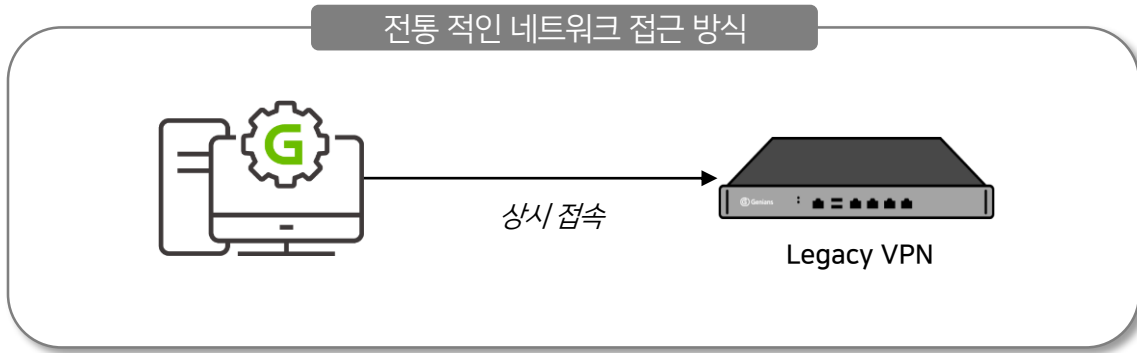
외부에 상시 오픈된 포트로 끊임 없는 공격

Brute Force, Credential Stuffing 인증 시도

VPN 인증을 우회하기 위한 다양한 해킹 시도

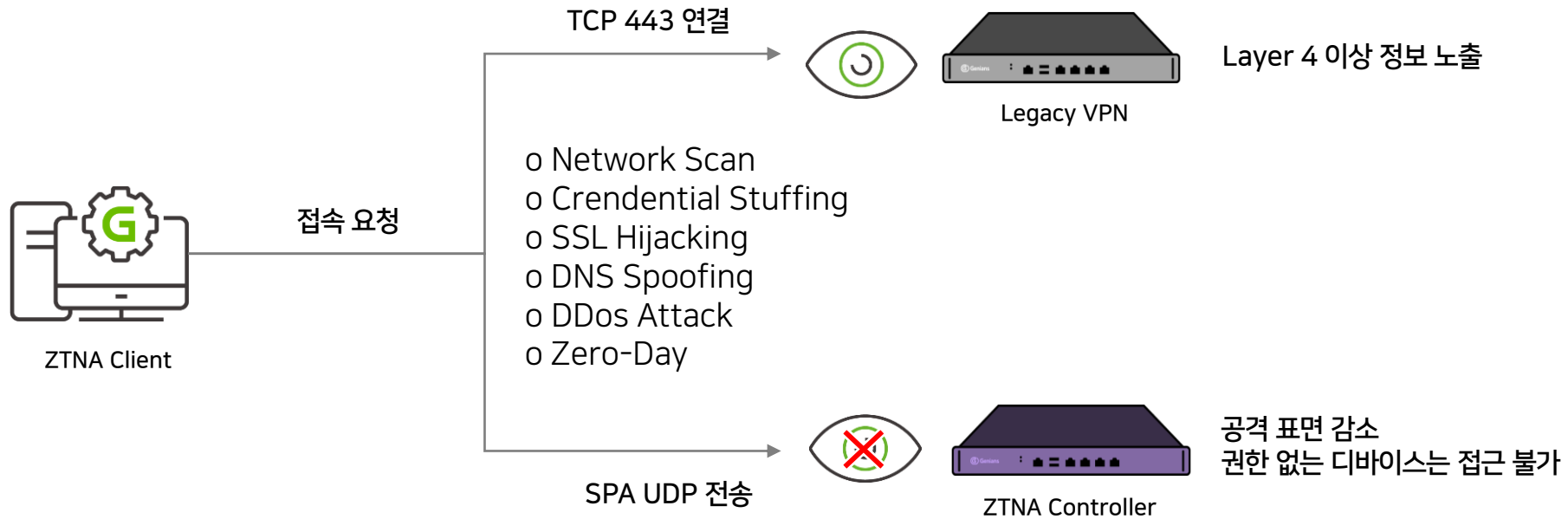
경계면 솔루션의 보안 취약점을 사용한 Zero Day 공격

소프트웨어 정의 경계 [VPN vs SDP]

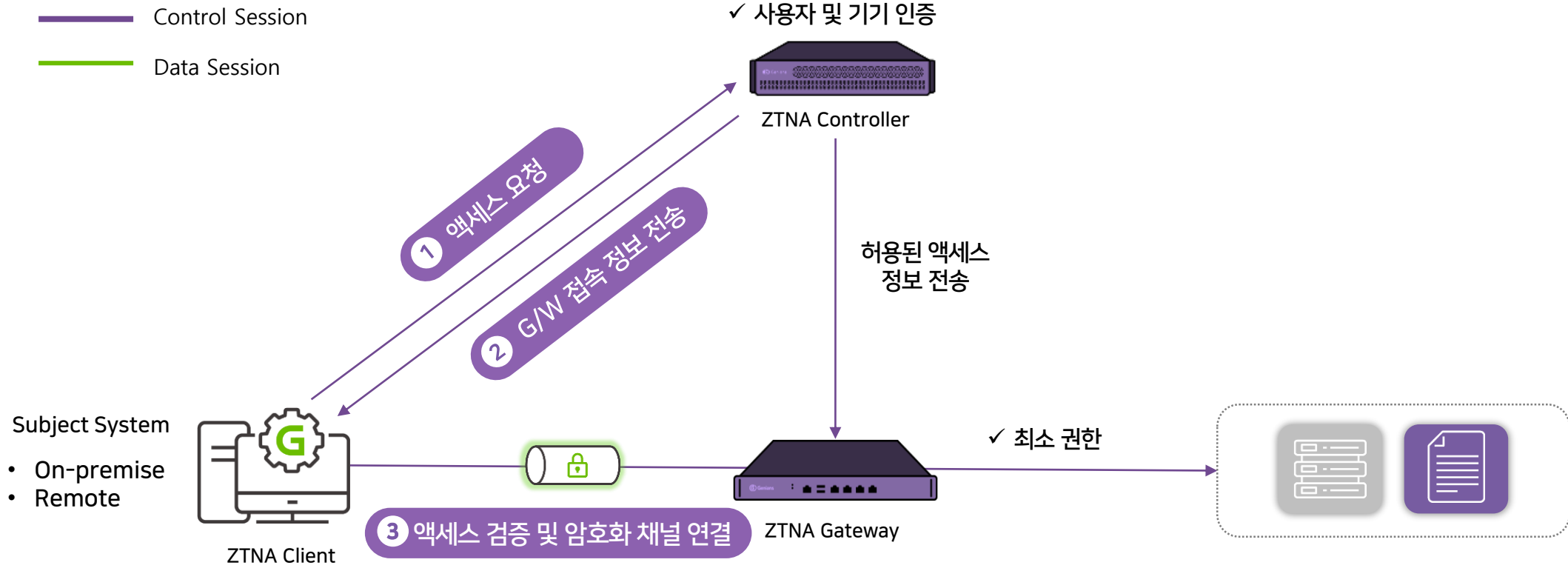


항목	SSL VPN	ZTNA
접근 방식	상시 서비스 접근 가능	√ 상시 서비스 접근 불가 (선 인증 후 네트워크 접근)
인증 방식	ID/PW+MFA 기반 인증	√ 사용자 및 기기 인증 (ID/PW+MFA, 기기 식별, 보안 검사)
접근 정책	네트워크 기반 접근	√ 사용자 중심 최소 권한 (IP주소 / 서비스 / 시간 / 어플리케이션)
세션 관리	최초 인증 후 지속적인 세션 유지	√ 지속적 신뢰 확인 (사용자, 장치 상태 실시간 평가)

- SPA(Single Packet Authorization) SDP 핵심 기술로 인가되지 않은 디바이스는 TCP 연결을 허용하지 않음




소프트웨어 정의 경계 [ZTNA SDP 연결 과정]



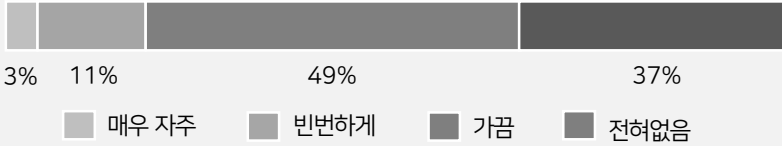
AS-IS

ID/PW 기반에 전통적인 인증 방식



기업 조직의 89%가 피싱 공격을 경험

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




3%	11%	49%	37%
매우 자주	빈번하게	가끔	전혀없음

* By HYPR, 2022 State of Passwordless Security Report

TO-BE

여러 단계의 보안 체인을 통해 네트워크 접근 과정에서 발생할 수 있는 보안 위험을 최소화



- ID/PW 외 MFA 적용
- 사용자 접속 위치

- 미확인 장치 접근 차단
- S/W 보안 취약점 관리
- 디바이스 상태 관리
- 업계 규정 준수
- 환경 요소

- 역할&속성 기반 정책 수립
- 허용되지 않은 애플리케이션 접근 차단
- 사용자/기기 상태 변경에 따른 적응형 정책
- 지속적 신뢰 평가



사용자 인증

동기화 및 인증 연동



ZTNA Center



인사DB



MySQL



ORACLE



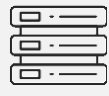
IBM
DB2



LDAP



SAML



RADIUS



REST API



다중 인증(MFA)

윈도우 Hello 및 애플 패스키 지원



PIN



Touch_ID



Face_ID



fido™
ALLIANCE simpler
stronger
authentication



SMS



구글OTP



WebHook



디바이스 인증

BYOD 단말 식별



Local CA 및 Unique-ID

보안 무결성 검사



기업 컴플라이언스 준수
(필수S/W, 보안패치, 업계 규정 등)

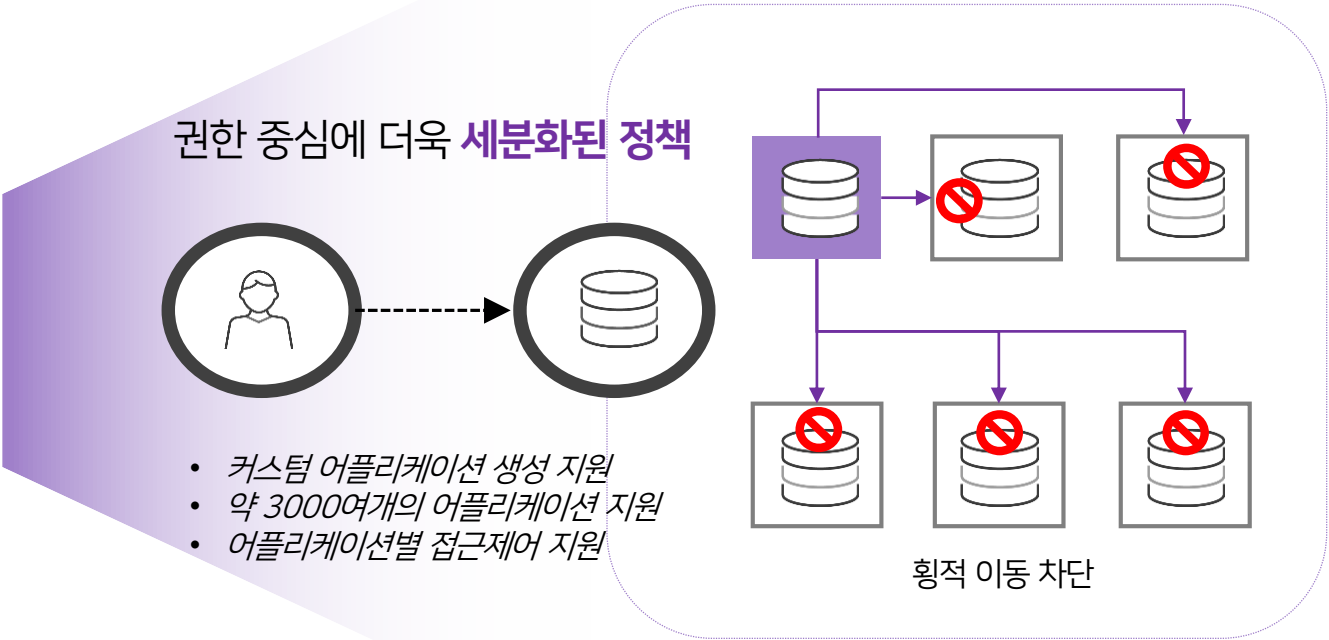
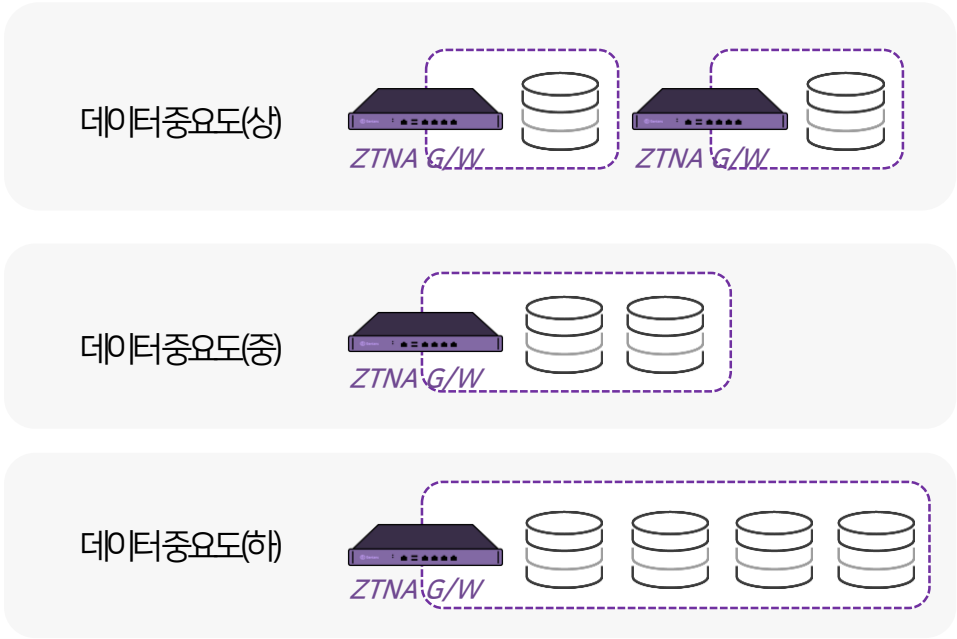
지속적 신뢰 확인



사용자 및 기기의 상태 변화에
따른 적응형 정책

마이크로 세그멘테이션 [네트워크]

- 위험 수준을 판별해 중요 자원은 ZTNA 에 보호되는 영역으로 분리하고 세분화된 액세스 정책을 적용해 내부에 침투한 공격자가 중요 리소스로 횡적이동 공격을 차단 및 위험 확산을 완화



마이크로 세그멘테이션 [가시성 & Context]

- 정책은 RBAC(역할) 뿐만 아니라 ABAC(위치, 역할, 시간, 장치 상태 등) 기반의 세밀한 접근 제어가 필요

네트워크 및 사용자 가시성

NT AG SS	동작	가용률	IP주소 수	MAC주소	NIC연더	제어정책	인증사용자	부서명	호스트명(이름)	등록시간	마지막 동작시간
	🟢	82%	10.11.0.8	2C:0D:A7:B6:F4:E5	Intel Corporate	Agent Not Installed	김승기	기술부/기술2팀	BOOK-IHARSPMCFG	2022-10-08 06:39...	
	🟡	76%	10.11.0.8	F8:E4:3B:09:0A:21	ASIX Electronics Cor...	Agent Not Installed	윤성복	기술지원센터/TAC2팀	YOON	2023-03-09 14:36...	
	🟡	13%	10.11.0.11	0C:9A:3C:E6:6A:B8	Intel Corporate	Agent Not Installed		DESKTOP-N2655J7		2023-02-20 14:15...	2023-03-17 00:23...
	🟡	0%	10.11.0.14	3CA6:F6:76:19:DB	Apple, Inc.	Agent Not Installed	김재현	기술연구소/Endpo...	3ca6:f6:76:19:db	2023-03-06 14:51...	2023-03-27 08:34...
	🟡	0%	10.11.0.36	A0:78:17:7F:BT:50	Apple, Inc.	Agent Not Installed	최정환	기술지원센터/TAC2팀	MACBOOK-PRO	2023-03-09 14:10...	2023-03-13 08:47...
	🟡	0%	10.11.0.37	00:E0:4C:68:00:3B	REALTEK SEMICOND...	User Not Authentica...		yckimui-MacBook...		2023-03-16 08:43...	2023-03-16 05:00...
	🟢	96%	10.11.0.40	A0:78:17:6D:3E:2B	Apple, Inc.	Default Policy	유동규	기술지원센터/TAC1팀	dgyru-macbookpr...	2022-11-24 15:05...	
	🟢	67%	10.11.0.44	8C:17:59:65:8F:10	Intel Corporate	Default Policy	조성문	DESKTOP-P3D8IAU		2023-02-24 16:07...	
	🟡	0%	10.11.0.50	02:27:02:02:0A:70	Unknown	Blocking Exceptions	윤성복	기술지원센터/TAC2팀	YOON	2023-02-27 14:26...	2023-02-28 00:51...
	🟢	57%	10.11.0.53	04:EA:56:3E:16:AB	Intel Corporate	Default Policy	문재훈	전달팀/전달팀2팀	GGMSOON2	2022-12-26 14:04...	
	🟢	44%	10.11.0.53	0C:D2:92:F8:4F:D5	Intel Corporate	Default Policy	박용우	지니언스(주)/인포...	0cd2:92:f8:4f:d5	2023-02-07 12:30...	
	🟢	99%	10.11.0.58	50:ED:3C:1F:6D:FB	Apple, Inc.	Block Exceptions (as...	이재욱	지니언스(주)/인포...	jws-MacBook-Air.1...	2022-12-20 12:13...	
	🟡	57%	10.11.0.62	F8:E4:3B:0F:7F:D8	ASIX Electronics Cor...	Default Policy	조성문	기술부/기술1팀	f8:e4:3b:0f:7f:d8	2023-01-11 17:24...	
	🟢	80%	10.11.0.66	88:E9:FE:79:A3:AC	Apple, Inc.	Default Policy	이소연	엔드포인트보안연구...	mouereui-MacBoo...	2023-02-28 20:00...	
	🟡	0%	10.11.0.72	E8:84:A5:2F:CF:0E	Intel Corporate	Blocking Exceptions	양선민	기술지원센터/TAC1팀		2023-03-22 14:45...	2023-03-23 05:00...
	🟢	96%	10.11.0.73	5C:91:E1:B5:22:27	Apple, Inc.	Default Policy	김용철	기술연구소/UX팀	yckimui-MacBook...	2023-03-15 10:38...	
	🟢	65%	10.11.0.75	8C:BB:7E:60:0F:BB	Intel Corporate	Default Policy	유현	엔드포인트보안연구...	L3IADK-C2	2022-10-07 09:57...	
	🟡	0%	10.11.0.77	E0:D5:5E:59:BC:3C	GIGA-BYTE TECHNO...	Blocking Exceptions	김대중	기술연구소/IP팀		2023-02-14 21:06...	2023-03-27 07:19...
	🟢	0%	10.11.0.78	70:A8:D3:13:2B:21	Intel Corporate	Default Policy	관한준	기술부/기술1팀	관한준	2022-12-13 10:23...	2023-03-15 07:26...
	🟢	79%	10.11.0.86	A0:78:17:69:B1:B1	Apple, Inc.	Default Policy	이준수	기술연구소/UX팀	leejsh-MacBookPr...	2023-02-14 10:59...	
	🟡	55%	10.11.0.94	A0:CE:C8:C1:E0:3E	CE LINK LIMITED	Default Policy	박용우	지니언스(주)/인포...	ab:ce:c8:c1:e0:3e	2023-03-02 11:06...	
	🟢	79%	10.11.0.105	E4:5E:37:A8:72:F8	Intel Corporate	Default Policy	김병준	엔드포인트보안연구...	LAPTOP-N8J49673	2022-08-29 13:52...	

트래픽 가시성

시간	출발지	목적지 Port	목적지	AS 조직명	목적지 Port	서비스	Application	호스트명	프로토콜	Packets	Bytes	동작	제어정책	사용자
2024-07-24 17:13:04	10.10.10.159	64225	8.8.8.8	GOOGLE	53	domain	Google		udp	2	140 B	Close	레이먼트/동작자단	harmony
2024-07-24 17:12:57	10.10.10.159	59857	184.29.17.18	AKAMAI-AS	443	https	WindowsUpdate	disc801.prod.do.dsp.mp.microsoft.com	tcp	13	2.4 KB	Close	harmony	harmony
2024-07-24 17:12:57	10.10.10.159	59860	172.16.25.18		443	https	TLS		tcp	14	2.47 KB	Close	harmony	harmony
2024-07-24 17:12:57	10.10.10.159	59865	20.49.150.24	MICROSOFT CORP MSN-AS-BLOCK	443	https	Microsoft	settings-win.data.microsoft.com	tcp	13	2.39 KB	Close	harmony	harmony
2024-07-24 17:12:57	10.10.10.159	49736	8.8.8.8	GOOGLE	53	domain	Bing		udp	2	256 B	Close	레이먼트/동작자단	harmony
2024-07-24 17:12:57	10.10.10.159	60242	8.8.8.8	GOOGLE	53	domain	Microsoft		udp	2	398 B	Close	레이먼트/동작자단	harmony
2024-07-24 17:12:57	10.10.10.159	59858	184.29.17.18	AKAMAI-AS	443	https	WindowsUpdate	disc801.prod.do.dsp.mp.microsoft.com	tcp	13	2.4 KB	Close	harmony	harmony
2024-07-24 17:12:57	10.10.10.159	59852	172.16.25.18		443	https	TLS		tcp	14	2.47 KB	Close	harmony	harmony
2024-07-24 17:12:57	10.10.10.159	59946	184.29.17.18	AKAMAI-AS	443	https	WindowsUpdate	kv801.prod.do.dsp.mp.microsoft.com	tcp	12	2.36 KB	Close	harmony	harmony
2024-07-24 17:12:57	10.10.10.159	59964	3.340.0.194	AMAZON-02	8443	psync-https	TLS		tcp	20	6.19 KB	Close	harmony	harmony
2024-07-24 17:12:57	10.10.10.159	59948	184.29.17.18	AKAMAI-AS	443	https	WindowsUpdate	disc801.prod.do.dsp.mp.microsoft.com	tcp	13	2.4 KB	Close	harmony	harmony
2024-07-24 17:12:57	10.10.10.159	59992	184.29.17.18	AKAMAI-AS	443	https	WindowsUpdate	kv801.prod.do.dsp.mp.microsoft.com	tcp	12	2.36 KB	Close	harmony	harmony
2024-07-24 17:12:57	10.10.10.159	59889	3.340.0.194	AMAZON-02	8443	psync-https	TLS		tcp	24	7.56 KB	Close	harmony	harmony
2024-07-24 17:12:57	10.10.10.159	61390	8.8.8.8	GOOGLE	53	domain	Google		udp	2	170 B	Close	레이먼트/동작자단	harmony
2024-07-24 17:12:57	10.10.10.159	59933	3.340.0.194	AMAZON-02	443	https	TLS		tcp	13	2.48 KB	Close	harmony	harmony
2024-07-24 17:12:57	10.10.10.159	59973	184.29.17.18	AKAMAI-AS	443	https	WindowsUpdate	kv801.prod.do.dsp.mp.microsoft.com	tcp	13	2.39 KB	Close	harmony	harmony
2024-07-24 17:12:57	10.10.10.159	60607	8.8.8.8	GOOGLE	53	domain	WindowsUpdate		udp	2	243 B	Close	레이먼트/동작자단	harmony

디바이스 가시성(Platform, Hardware, Software, Update..)

IP 주소: 10.64.0.2 [DHCP]

IPv6 주소: DOWN

관리센터: S-10.64.0.1

스위치(포트): 10.64.0.1 (0)

NATed IP: 43.200.194.48/37480

최초 등록: 2023-03-27 09:41:47

마지막 동작시간: 2023-03-27 09:51:02

MAC 주소: 00:E0:4C:68:00:17

IPv6 링크로컬: 가상

장비: 10.64.0.2 (2/3)

접속AP: 없음

NAT 장비: 지정

가동률: 63.00%

최근 노트 검사: 2023-03-27 09:41:47

호스트명	제품 버전	현재버전 버전명	현재버전 날짜	실시간시	최근검사시간
Windows Defender	4.18.2201.11	1.385.1197.0	2023-03-27 00:55	동적	2023-03-22 11:44

소프트웨어목록	프로그램명	버전	경로
AnySign4PC	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_srvc_2407	
Canon Office Printer Utility	12.7.0.0	C:\Program Files\WindowsApps\34791E63.CanonOfficePrinterUtility_12.7.0.0_x64_6e5878c60951	
CapturePicker	10.0.19580.1000	C:\Windows\SystemApps\Microsoft.Windows.CapturePicker_cw5n1h2zyewy	
Chrome	111.0.5563.111	C:\Program Files\Google\Chrome\Application	
Clicchamp	2.5.15.0	C:\Program Files\WindowsApps\Clicchamp.Clicchamp_2.5.15.0_neutral_yxz26nhtzhrt	
ColorDirector for LGE	5.0.8107.0	C:\Program Files\WindowsApps\www.cyberlink.com.ColorDirectorforLGE_5.0.8107.0_x64_srvc	
Cortana	4.2204.13303.0	C:\Program Files\WindowsApps\Microsoft.549981C3F5F10_4.2204.13303.0_x64_8wekyb3d8bbwe	
DTXs.Ultra	1.11.11.0	C:\Program Files\WindowsApps\DTXInc.DTXUltra_1.11.11.0_x64_152f2b0d937r	

호스트명	리버전	메타데이터	종도	CPU 사용량	
tronics	12th Gen Intel(R) Core(TM) i7-1265P	Intel Corporation	591523	준제함	1.88%

클라우드 가시성

NT AG SS	동작	IP주소 수	MAC주소	플랫폼	호스트명(이름)	장비명 / 센서명	등록시간
	🟢	10.1.124.22	26:A0:09:2F:D7:A5	(Tech)		tech.demo.genians.co.kr /	2022-12-22 09:45:11
	🟡	192.168.0.126	02:EB:DE:0F:42:66	Ubuntu Linux 20.04	Genian ZTNA Cloud Se...	SW-10.1.124.22 / Tech	2023-03-04 14:24:43
	🟢	192.168.2.213	02:F2:BF:47:C4:E2	Ubuntu Linux 20.04	Genian ZTNA Cloud Se...	SW-10.1.124.22 / Tech	2023-02-20 16:31:27
	🟡	192.168.7.54	02:D9:1D:0D:5F:28	Ubuntu Linux 20.04	Genian ZTNA Cloud Se...	SW-10.1.124.22 / Tech	2023-01-03 14:37:36

CLOUD TYPE

Cloud 정보 / 값이면 (Object/Value)

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.CustomerOwnedIpv4	
aws.Address.PrivateIpv4Address	"192.168.2.213"

2	1	2
cloud T2micro	cloud T2medium	cloud T2large

마이크로 세그멘테이션 [분류 & 권한]

- 필요한 시간(Just-In-Time)에 필요한 만큼(Just-Enough) 권한을 제공하기 위해 대상을 분류하고 권한을 정의

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

IP/MAC	등록일자	노트 타입	트래픽	시스템 정보
Agent 상태	Platform	백신 정보	사용자 계정	열린 Port
Update 정보	어플리케이션	Tag	On/Off	패스워드



✓ 사용자 중심에 적시에 필요한 최소 권한을 부여

	네트워크 객체	서비스 객체	시간 객체	어플리케이션 객체
<input type="checkbox"/>	NET-ALL	ALL	ANYTIME	ALL
<input type="checkbox"/>	PERM-INTERNET	EXCLUDE MANAGED	ANYTIME	ALL
<input type="checkbox"/>	PERM-LOCAL	LOCAL	ANYTIME	ALL
<input type="checkbox"/>	PERM-MANAGED	MANAGED	ANYTIME	ALL
<input type="checkbox"/>	PERM-WEB1	web1	ANYTIME	ALL
<input type="checkbox"/>	PERM-WEB2	ALL

권한 조합

IP 주소 | **TCP/UDP 서비스**

IP/Netmask: 10.254.10.0/255.255.255.0 | 프로토콜: ALL | TCP/UDP: 80, 443

시간 | **어플리케이션**

모든날짜 | Application ID: Genians | Match Rule: www.genians.com, www.genians.co.kr, docs.genians.com

마이크로 세그멘테이션 [제어 정책]

- 분류 대상(그룹)은 정의된 제어 정책에 의해 규정을 만족해야만 허용된 서비스(최소 권한) 에 접속할 수 있는 권한을 획득

<input type="checkbox"/>	순서	ID	노드수	사용	노드그룹	권한객체
규정 (Compliance) ⓘ						
<input type="checkbox"/>	1	예외허용		<input checked="" type="checkbox"/>	예외노드	PERM-ALL
<input type="checkbox"/>	2	IP관리 차단		<input checked="" type="checkbox"/>	IP관리 차단노드	PERM-DENY
<input type="checkbox"/>	3	미인증차단	2	<input checked="" type="checkbox"/>	미인증노드	PERM-DENY
보안성 검사		DeviceID 미할당 노드 차단		<input checked="" type="checkbox"/>	DeviceID미발급	PERM-DENY
		TrustScore 안전 점수 미달 노드 차단		<input checked="" type="checkbox"/>	Trustscore 0-500점	DENY-ICAM
권한 (Permission) ⓘ						
최소 권한		시스템관리자	1	<input checked="" type="checkbox"/>	시스템 운영부	서버
		일반사용자		<input checked="" type="checkbox"/>	임직원	그룹웨어
		개발자	1	<input checked="" type="checkbox"/>	개발부서	개발서버
		기본권한정책	1	<input checked="" type="checkbox"/>	모든노드	PERM-DENY

“제로트러스트 원칙의 최소 권한 할당을 위해 White List 방식에 제어 정책 수립”



1. 규정(Compliance)

- 네트워크에 접근하는 모든 노드들이 준수해야 하는 규정을 정의



2. 권한(Permission)

- 규정을 준수한 노드들이 접근할 수 있는 서비스에 대해 정의

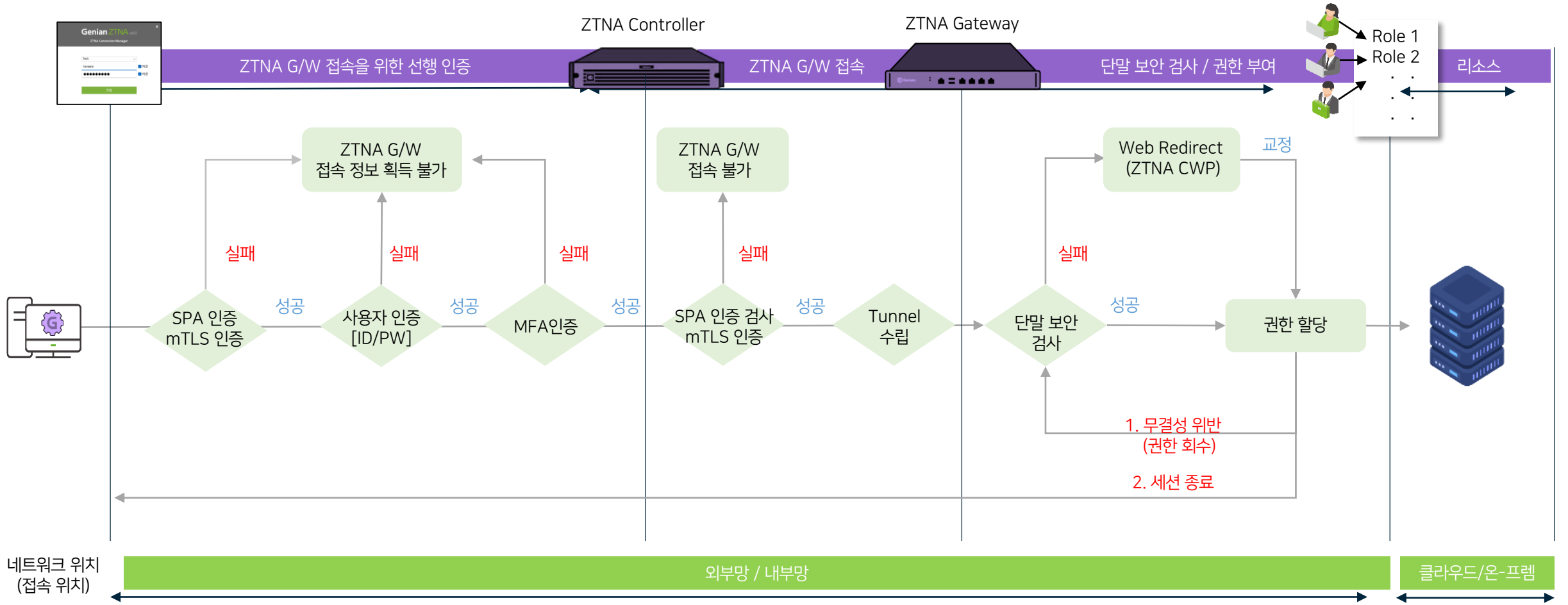
사용자	규정 정책	권한 정책				허용 서비스		허용 어플리케이션	
		접속 위치	자산 유형	플랫폼	업무 시간				
일반 사용자	기본 보안 설정 필수 소프트웨어 보안 패치	사무실	PC	Windows	평일 09:00-18:00	그룹웨어	192.168.10.10:443	ERP	www.erp.com www.erp.com/home
						파일서버	192.168.10.11:80		
시스템 관리자	기본 보안 설정 필수 소프트웨어 보안 패치	재택	PC	MAC OS Windows	상시 00:00-24:00	원격 접속	10.22.10.10:3389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

마이크로 세그멘테이션 [조건부 액세스 및 동적 접근 제어]

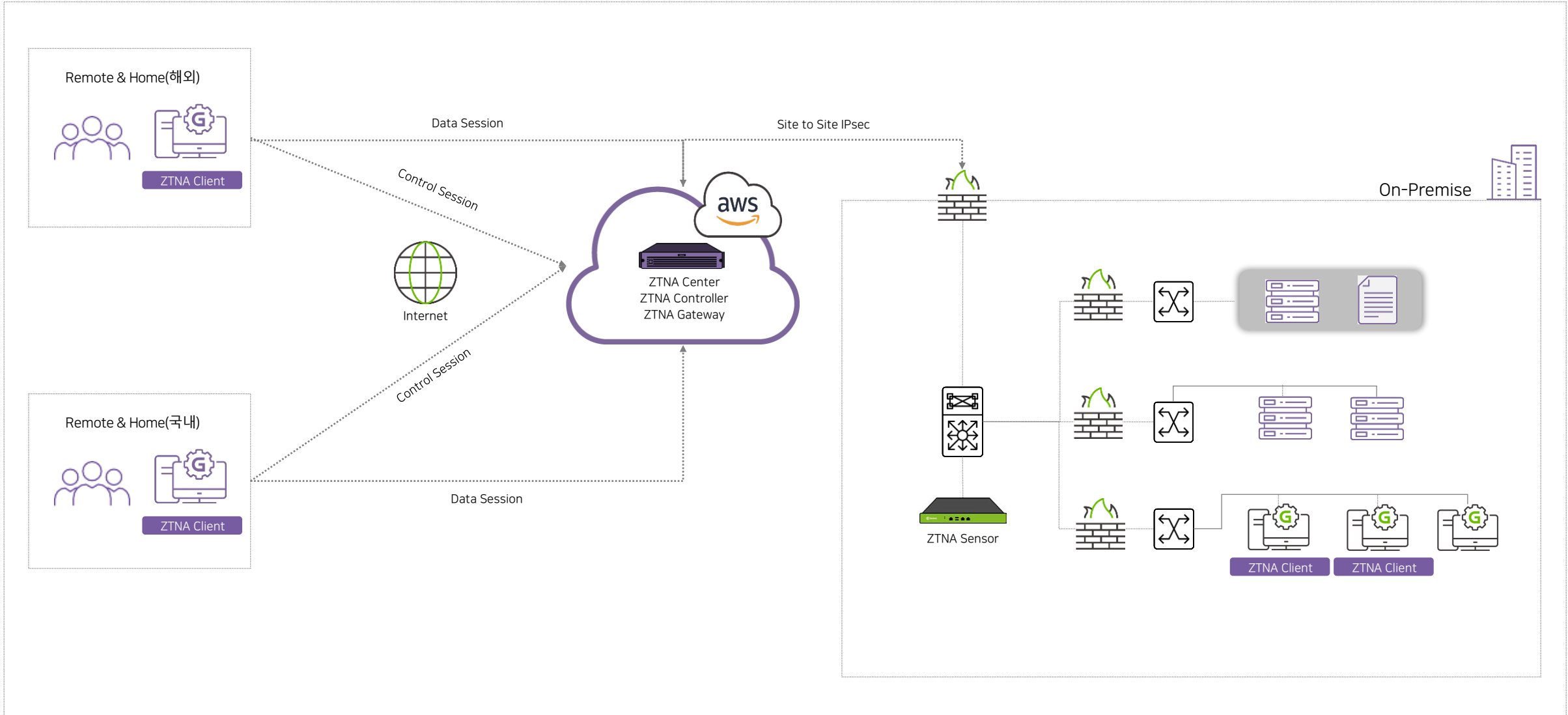


- 💡 사용자에게 알림
(차단 웹, 에이전트 팝업, 인스턴스 메시지)
- 관리자에게 알림
(특정 이벤트 발생 시 SMS, E-mail 발송)
- 특정 로그 외부 전송
(타 보안 솔루션으로 로그 전송하여 모니터링)
- ⊗ 조건에 따른 네트워크 차단
(신규 IP/MAC, 미 인증, 보안 설정 위반 등)
- 특정 프로세스 중지
(관리자가 지정한 프로세스)
- USB 장치 차단
(USB 저장 장치 등 강제 Off)
- ✔ 필수 SW 설치 유도
(백신, DRM 등 보안 솔루션 강제 설치)
- 불법 SW 삭제
(허용되지 않은 특정 SW 강제 삭제)
- 보안 설정 강제화
(패스워드 설정, 화면보호기 등)

Genian Cloud ZTNA 접속 개념도



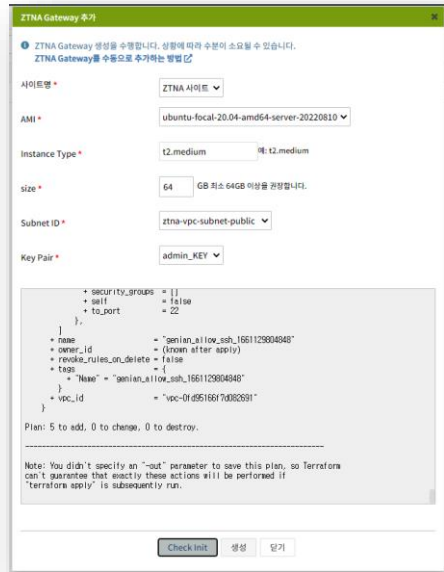
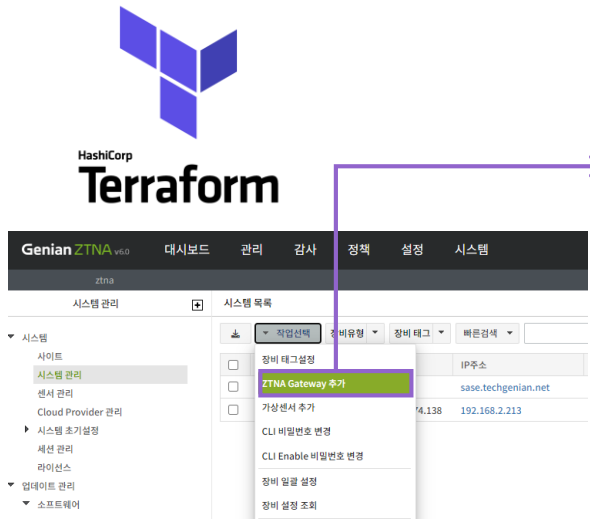
Genian Cloud ZTNA 아키텍처



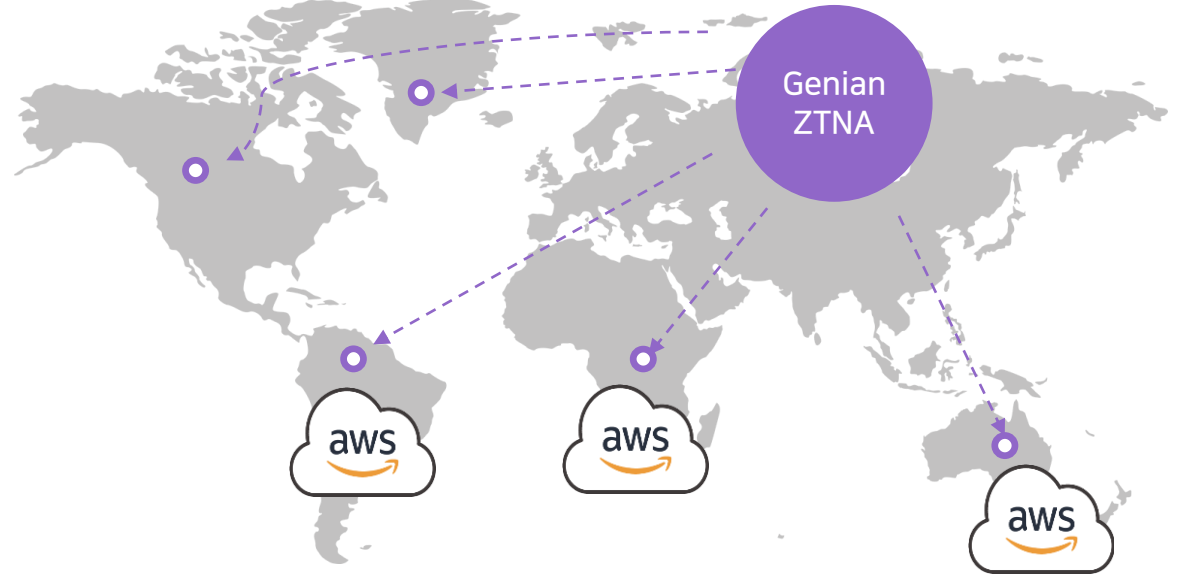
03.

Cloud ZTNA 활용 방안

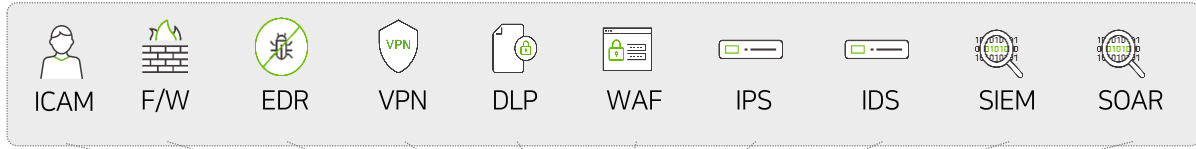
자동화 및 오케스트레이션



클라우드 PoP 을 통한 해외 지점 관리



3rd Party 제품 연동



고객이 보유한 다양한 3rd Party 보안 제품

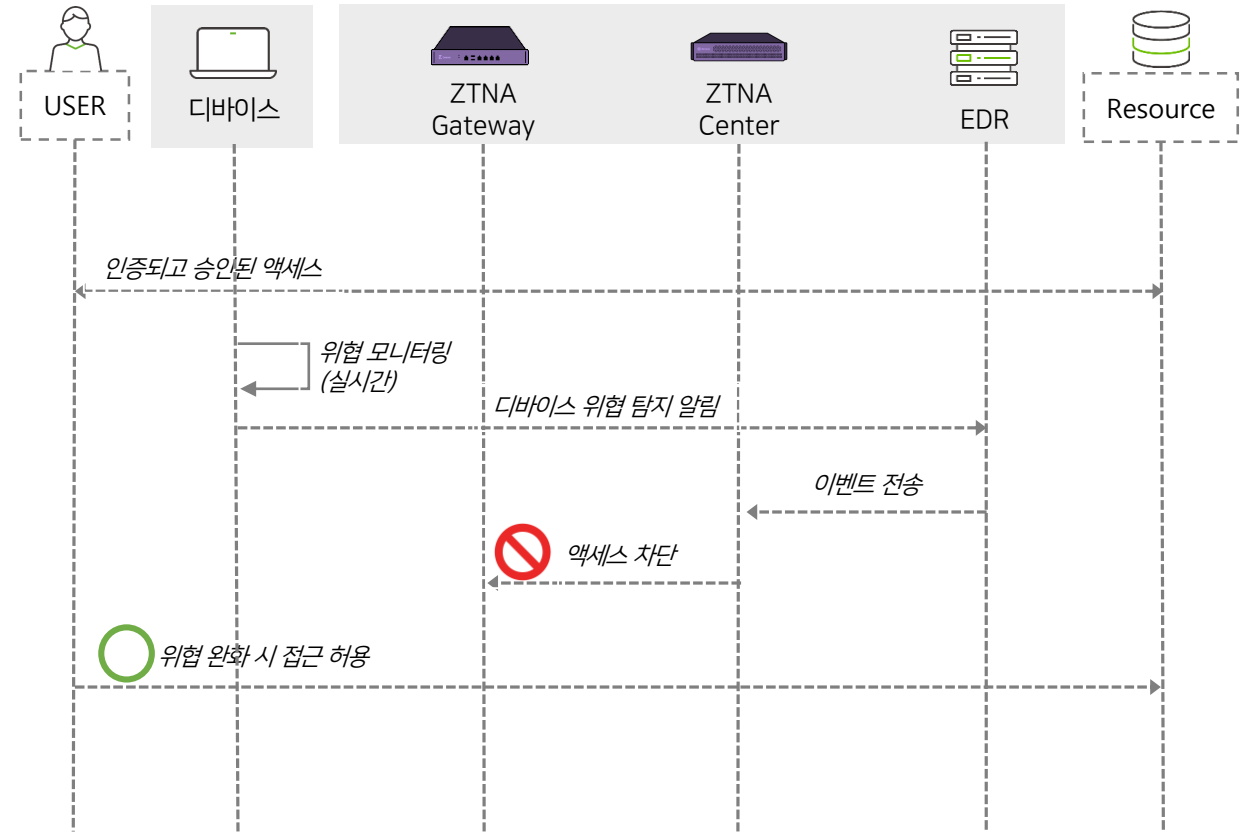
WorkFlow 를 통한 보안 자동화 관리

연동 정보
 각 프로세스에서 공통으로 사용하는 값을 정의해서 사용할 수 있습니다.
 예) Request URL

Params
 apiKey 483afe222-2ch6-4h4d-81...

#1 #2 #3 (Workflow configuration panels with Name, Request URL, Method, Headers, Body, Response Type, and Response Body Template fields)

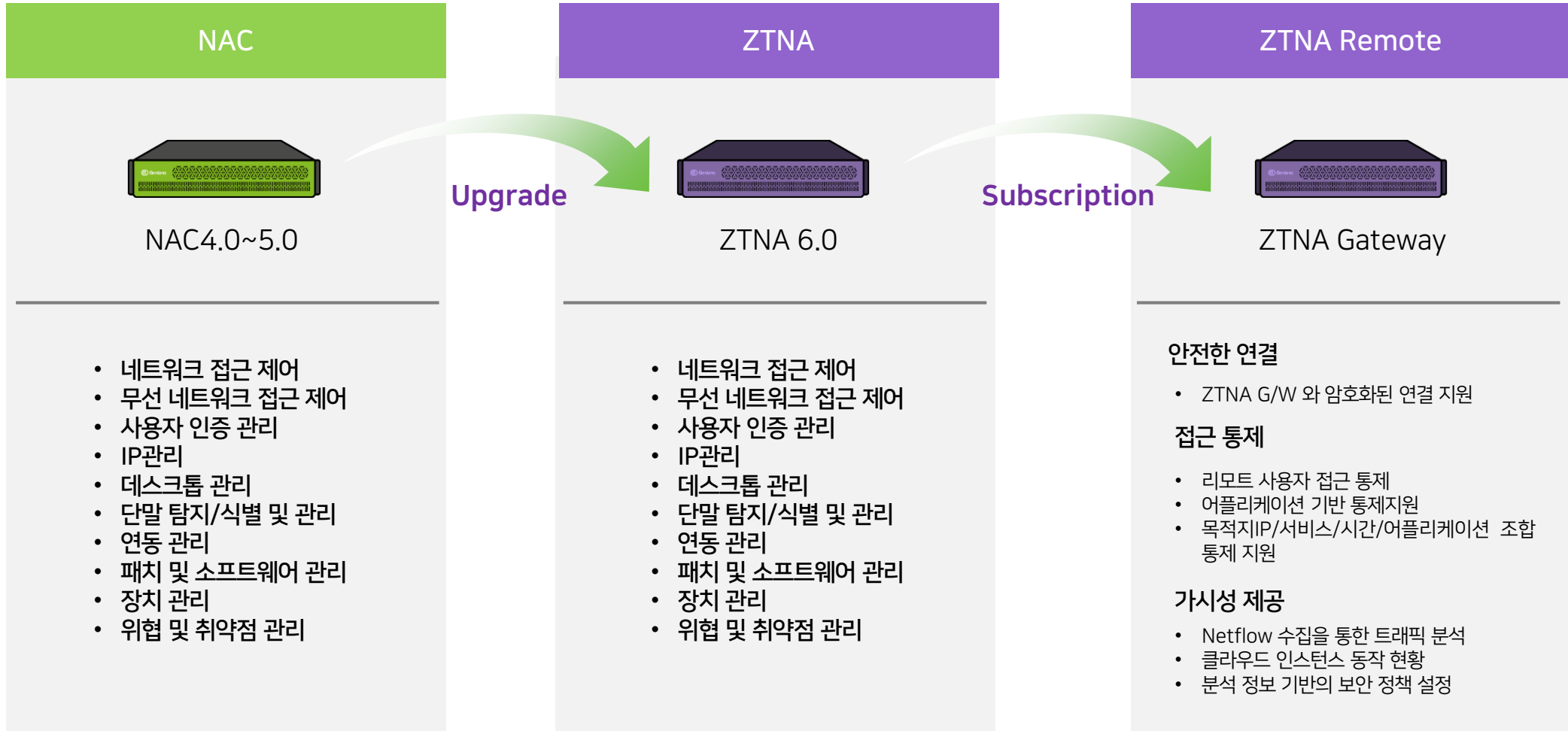
Radius Syslog API SNMP WEBHOOK SAML Terraform

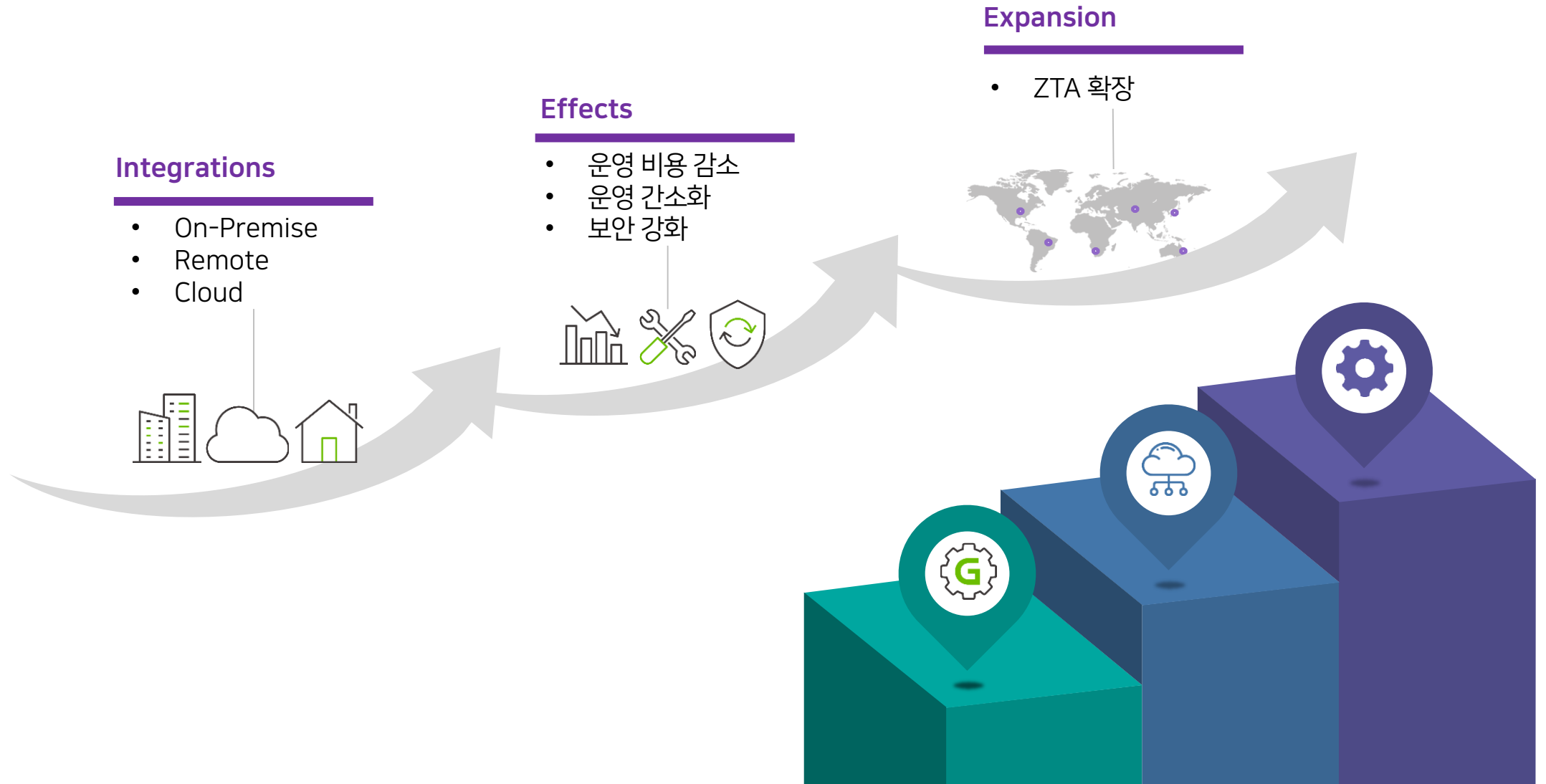


3rd party 솔루션 연동 시나리오

04.

Summary





통합 보안 플랫폼 기업, 지니언스

THANK YOU :)