

Intelligent **Zero Trust** Network Access

망분리 규제 완화와 제로 트러스트

2024. 10



CONTENTS

01. ZTNA 가 필요한 이유

02. APPLICATION iNSIGHT ZTNA

01

ZTNA 가 필요한 이유

Perimeter Security Model

→ Zero Trust Security Model의 재조명

“ Zero Trust : 신뢰하지 않고 항상 확인 한다”

네트워크 내부와 외부 구분하지 않고

- 모든 접근 요청에 대해 신원을 확인하고 권한을 검증
- 사용자가 필요한 최소한의 권한만을 부여
- 접근이 허가된 후에도 활동에 대한 지속적인 모니터링과 검증

Digital Business Transformation

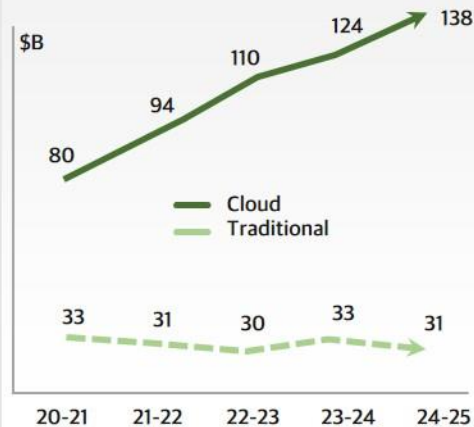
→ 디지털 전환으로 인한 업무 환경의 변화

하이브리드 형태 근무 증가



전 세계 지식 근로자 중
하이브리드 근무 비중 → **3배** 이상 증가

기업의 클라우드 도입 증가



클라우드 도입 상승



전통적인 제품과
클라우드 제품의
경계가 흐려짐

- 디지털 비즈니스 전환으로 인한 재택 근무, 하이브리드 업무 환경의 증가
- 사용자, 디바이스, 애플리케이션, 데이터가 기존의 데이터센터를 떠나

기업 경계와 통제 영역 밖에 위치

Expanded the Attack Surface for Attackers

→ 변화하는 디지털 환경에 따른 공격 표면 증가

다양한 접근 지점



다양한 디바이스 사용

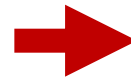


+

클라우드 도입 증가



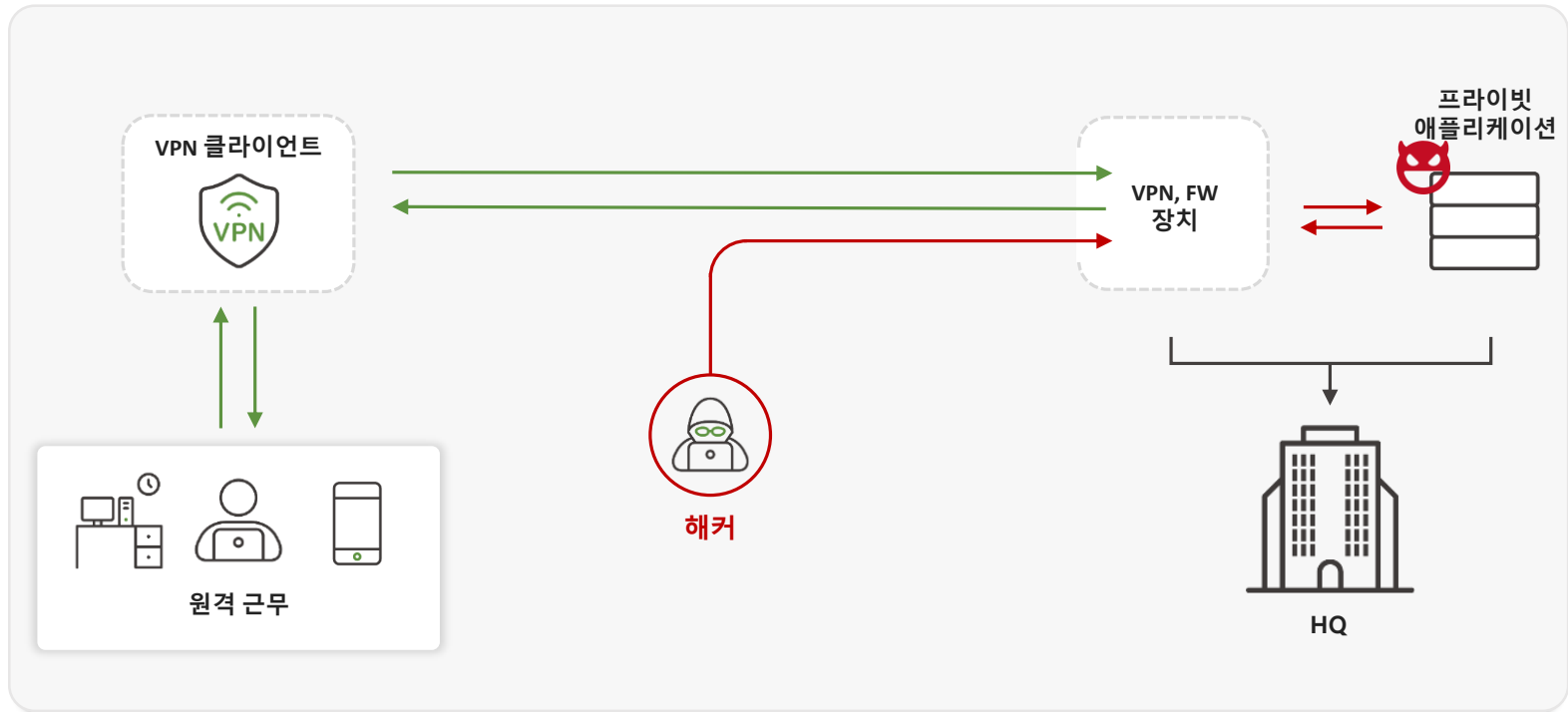
보안 인식 부족



공격 표면의 확장으로 인한
잠재적 보안 위협 증가

Legacy Networking and Security Approaches Have Become Ineffective

→ 기존 보안 접근 방식(VPN)의 결함과 한계



기존 VPN은 사용자가 네트워크에 연결되면 모든 기업 리소스에 대한 '무제한 액세스 권한'을 부여



기업의 중요 리소스, 애플리케이션에 제한 없이 액세스할 수 있기 때문에 Lateral Movement같은 공격에 취약한 상태로 머물러 '더 큰 데이터 유출을 초래'

VPN Vs ZTNA

특징	전통적인 VPN 솔루션	ZTNA 솔루션 (On-premise)
접근 방식	네트워크 중심 (기업 네트워크 전체에 접근 가능)	애플리케이션 중심 (특정 리소스에만 접근 가능)
접근 권한	광범위한 접근 권한 (네트워크 전체에 대한 접근 가능)	최소 권한 원칙 (필요한 리소스에만 접근 허용)
인증 방식	단일 사용자 인증	다중요소 인증 (MFA) 및 컨텍스트 기반 인증
공격 표면	넓은 공격 표면 (네트워크 전체가 노출됨)	제한된 공격 표면 (특정 리소스만 노출됨)
세분화된 접근 제어	제한 (네트워크 수준에서 접근 제어)	세분화된 접근 제어 (애플리케이션 수준에서 접근 제어)

공공기관 망분리 규제 완화

뉴스

• 관련도순 • 최신순 | 모바일 메인 언론사 ☐

뉴스 PICK • 6일 전 • 네이버뉴스

윤오준 국정원 3차장 "공공망 분리 제도 개선, '보안 약화' 해석...

이른바 '다중계층보안(Multi Level Security, **MLS**)'을 도입하는 것이다. 이를 통해 내·외부를 경계하는 형태의 보안이 아닌 데이터 중심의 보안 체계로 전환하는... 국정원은 이를 통해 인공지능(AI)·빅데이터 등 신기술을 ...



머니투데이방송 • 1주 전

망분리 규제 완화 첫발...MLS 신시장 열린다

MLS 구현을 위해 최근 중요성이 높아지고 있는 제로 트러스트 보안 모델이 적용됩니다.국정원 **MLS** TF의 한 관계자는 제로트러스트는 아무도 신뢰하지 않는다는 원칙을 구현하기 위한 기술이라며, 새로운 국가 사이...



전자신문 PICK • 1면 TOP • 3주 전 • 네이버뉴스

2026년부터 공공기관 'PC 1대로 업무'...국정원, 물리적 망분리 ...

국정원, **MLS** 가이드라인 준비 VDI-제로트러스트 신기술 활용 C-S-O 데이터 등급서 'I' 추가 내부망과 인터넷망 접속 가능 국가정보원이 2026년 국가-공공기관에서 한 대의 개인용컴퓨터(PC)로 모든 업무를 볼 수 있도록...



전자신문 • 2면 3단 • 2024.04.01. • 네이버뉴스

국정원, 망분리 개선 로드맵 9월 발표...'MLS TF' 띄운다

국정원은 **MLS** 전환을 통해 망분리 체계를 개선하고 데이터 활용과 보안성 두 마리 토끼를 잡을 방침이다. 분과별로 **MLS** 체계 기밀 개선 분과는 **MLS** 전환 이후 보안 체계 내 기밀 데이터를 분류하는 기준을 수립하고...



- 현황 및 문제점
: 물리적 망 분리는 PC 2대를 사용해야 하는 업무 /비용 효율이 낮고 AI, SaaS등 신기술 보급 확산에 걸림돌
- 목표
: PC 1대로 내/외부망 업무 수행
VDI 및 제로트러스트 등 망 분리를 보완하기 위한 기술 채택
예) SWG+RBI / ZTNA
- 추진경과(2024~)
: 국가 사이버보안 체계를 다중계층보안 MLS(Multi Level Security)로 전환
- 향후 계획
: MLS 가이드라인 1.0 초안 공공기관 공유(2024.9)

금융기관 망분리 규제 완화 - 망분리 규제 개선 로드맵 주요 내용

- 연구개발 업무의 효율성 제고를 위해 망분리 예외 허용
 - ◆ 개인신용정보 활용하지 않는 연구개발
 - ◆ 업무에 한해 물리적 망분리 예외 허용
- 망분리 예외에 따른 보안성 확보를 위해 부가조건
 - ◆ 유해 사이트 차단 등 접근 통제 정책 등
 - ◆ 독립적인 네트워크 구성
- 비중요업무에 한해 내부망의 SaaS 이용 허용
- 내부망 사이버침해 예방등을 위한 보안 부가조건
 - ◆ SaaS 안정성 평가
 - ◆ SaaS 이용에 따른 필요 보안대책 수립
- 생성형 AI 활용 – 현재는 보수적 활용
 - ◆ 개인정보 가명화를 통한 활용 방안

이용업무 범위확대

생성형AI 및 SaaS 규제 특례
정규제도화

자율보안-결과책임 원칙
신 금융보안체계 구축

02

APPLICATION *i*NSIGHT ZTNA

AIONCLOUD (구독형 서비스)

Website Protection

→ 웹 프로덕션 인프라에 대한
보안 서비스



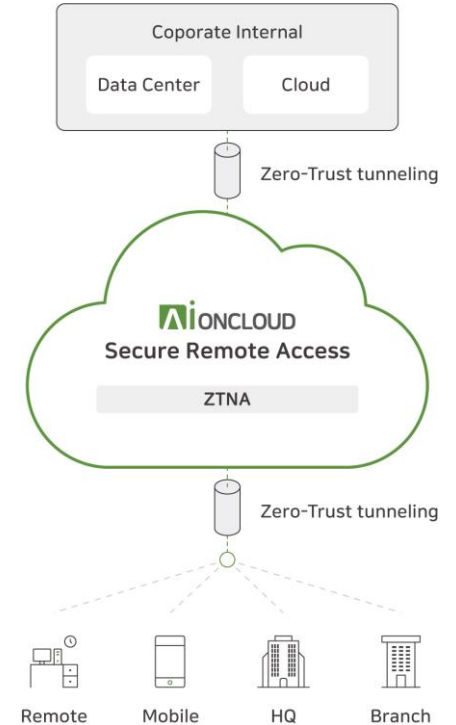
Secure Internet Access

→ 직원의 안전한 인터넷 연결을 보장하는
SSE 서비스



Secure Remote Access

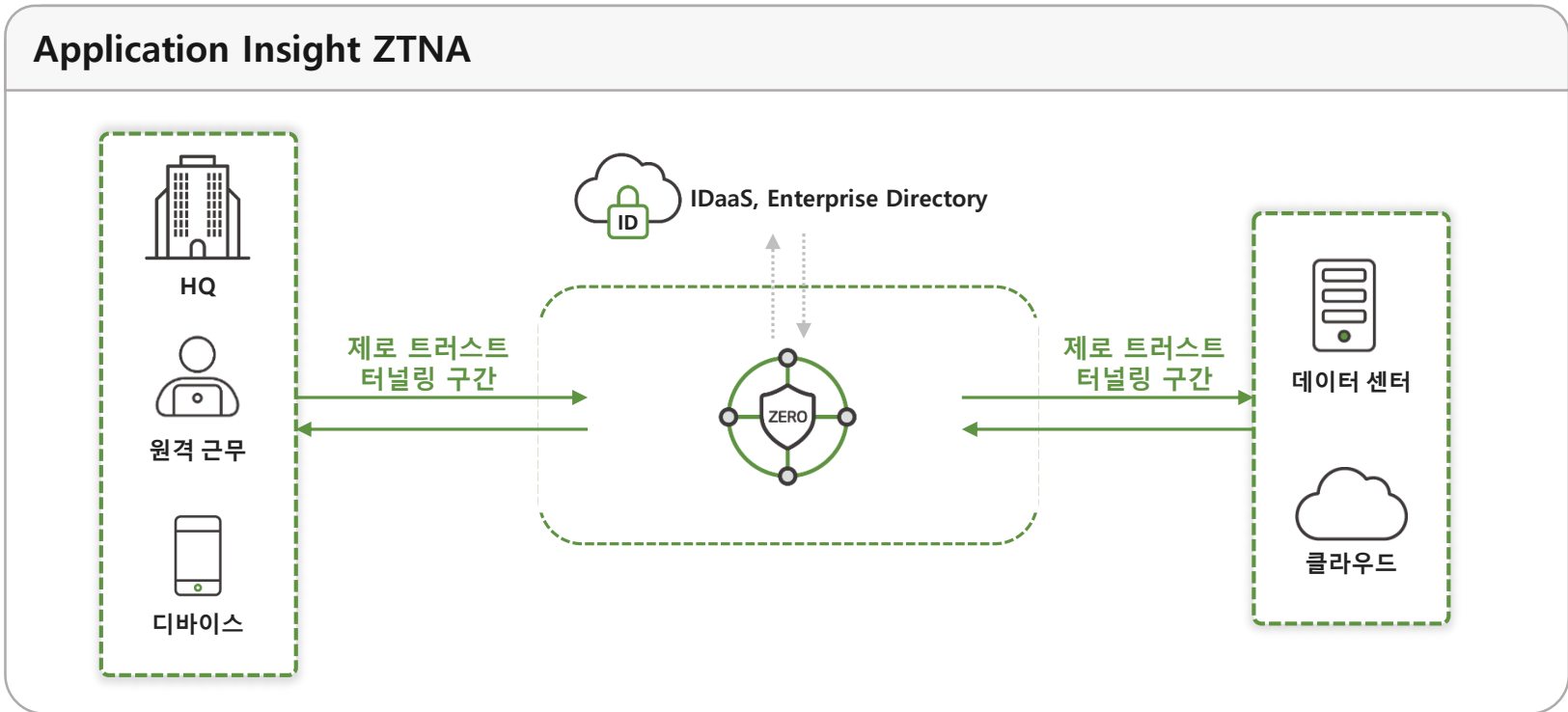
→ 직원과 기업 애플리케이션간
제로 트러스트 보안 서비스



AIZTNA Overview

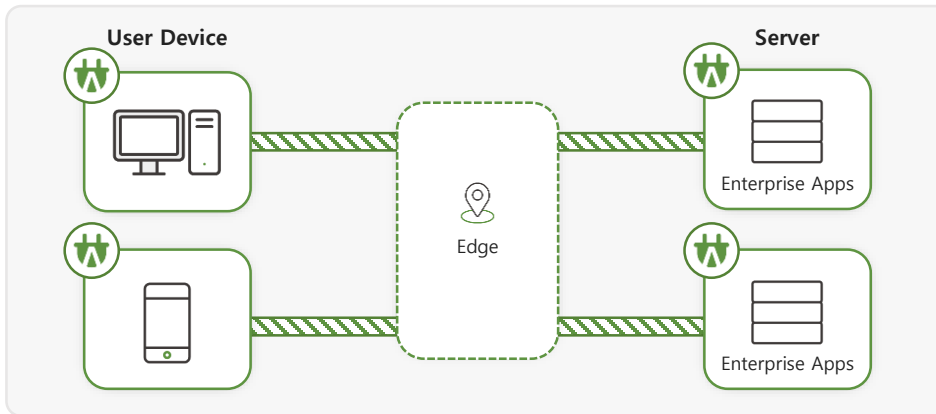
사용자와 기업 애플리케이션 간의 안전한 접근을 보장하는 'ZTNA' 솔루션

- 기존 네트워크 변경 없이 AIConnector를 통해 기업 애플리케이션 트래픽만 Edge로 터널링
- 기업 애플리케이션 연결과 인터넷 다이렉트 트래픽에 대한 사용자 경험 보장
- 신원 및 컨텍스트를 기반으로 언제 어디서든 사용자 중심의 일관된 보안 정책 적용



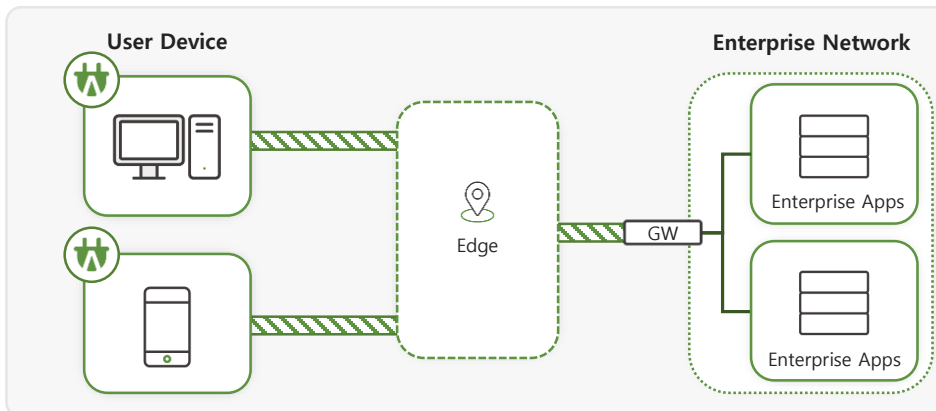
Configurations

1 'AIConnector for Client' to 'AIConnector for Server'



- 사용자 디바이스별 커넥터 배포 및 Edge 터널링
- 서버별 커넥터 배포 및 Edge 터널링
- 낮은 지연 시간 및 풍부한 보안 기능 제공
- Full Zero Trust Tunneling을 통한 높은 보안 성능과 세밀한 액세스 제어, 가시성 확보 가능

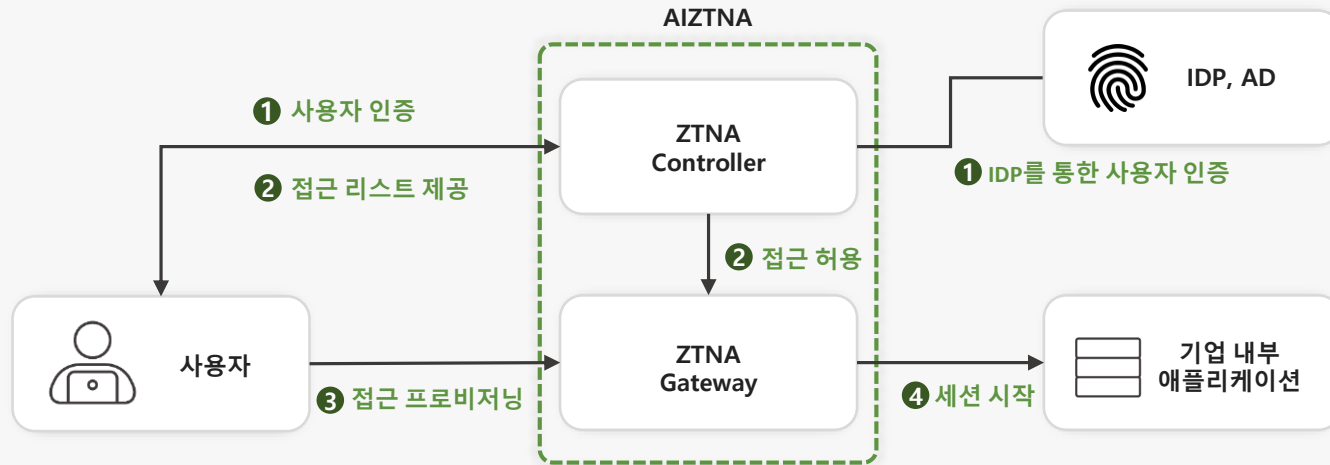
2 'AIConnector for Client' to 'Gateway Connector'



- 사용자 디바이스별 커넥터 배포 및 Edge 터널링
- 기업 네트워크에 게이트웨이 커넥터 배포 및 Edge 터널링
- Edge와 게이트웨이 커넥터 간 단일 터널 생성 및 관리
- 다양한 서버 리소스에 대한 통합 액세스 제어에 효과적 구성

How It Works

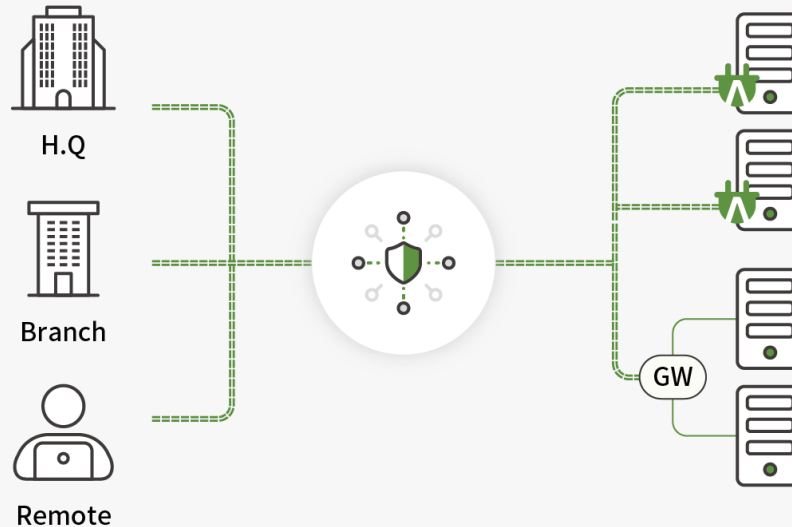
사용자와 리소스의 직접 연결로 제로 트러스트 보안 구현



- 1 OKTA, Entra ID 등 IDaaS 및 Active Directory 통합을 통한 사용자 인증
- 2 사용자, 디바이스, 그룹 별 접근 권한 애플리케이션 리스트를 전달하고, 해당 사용자의 기업 내부 애플리케이션 접근 정보를 전송
- 3 사용자 디바이스에 설치된 AIConnector(agent)를 통한 Posture check 수행 및 최소 권한 접근 허용, 혹은 웹 브라우저에서 실행되는 Application Launcher(agentless)를 통한 제한적인 접근 허용
- 4 클라이언트용 AIConnector와 서버 게이트웨이 혹은 서버에 설치된 서버용 AIConnector를 통한 안전한 제로 트러스트 터널 설정
- 5 클라이언트와 Edge 간, 서버와 Edge 간 양방향 터널을 결합하고 오가는 모든 트래픽 검사하여 사용자나 디바이스로부터 발생하는 잠재적인 위협을 감지하고 차단

Features & Benefits

Full tunneling 기반의 안전한 접속 환경 제공



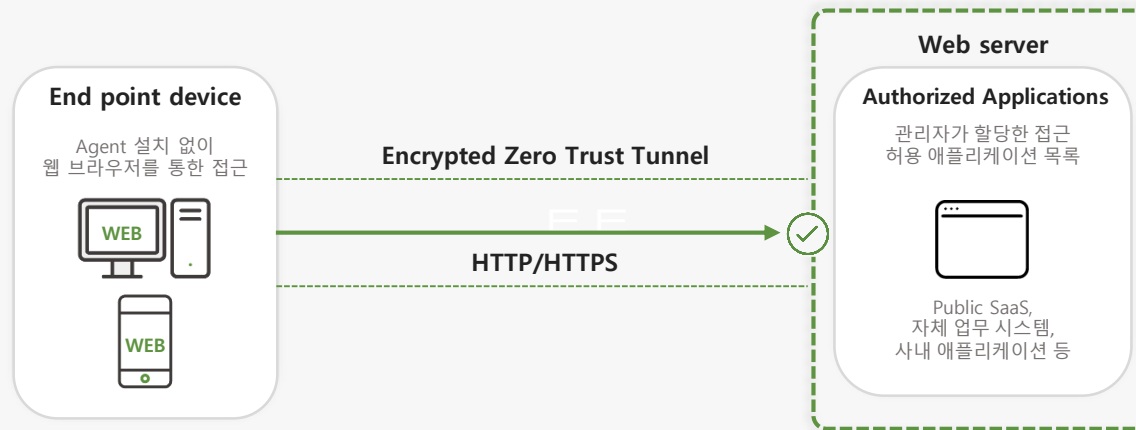
- SDP(Software Define Perimeter) 기반으로 신원과 맥락이 확인된 사용자만 기업 애플리케이션에 접근
- 퍼블릭 네트워크에 노출되지 않는 **User-to-App 직접 연결**(서버 에이전트 & 게이트웨이 커넥터 지원)
- 다양한 엔드포인트 디바이스와 애플리케이션 서버 환경 지원

AIconnector for Client : Windows, macOS, iOS, Android

AIconnector for Server : Windows server 64bit, Ubuntu, Red Hat Enterprise Linux / CentOS

Features & Benefits

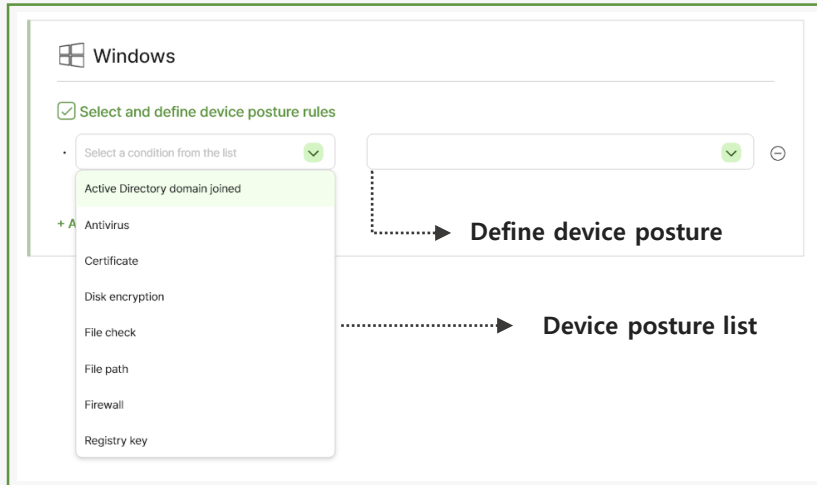
Application launcher을 통한 애플리케이션 직접 연결



- **AIConnector less** 환경에서 기업 애플리케이션에 접근할 수 있는 Application Launcher 제공
- 퍼블릭 네트워크에 노출되지 않는 FQDN 관리 및 TLS 기반의 안전한 접근 보장

Features & Benefits

End-point device posture check

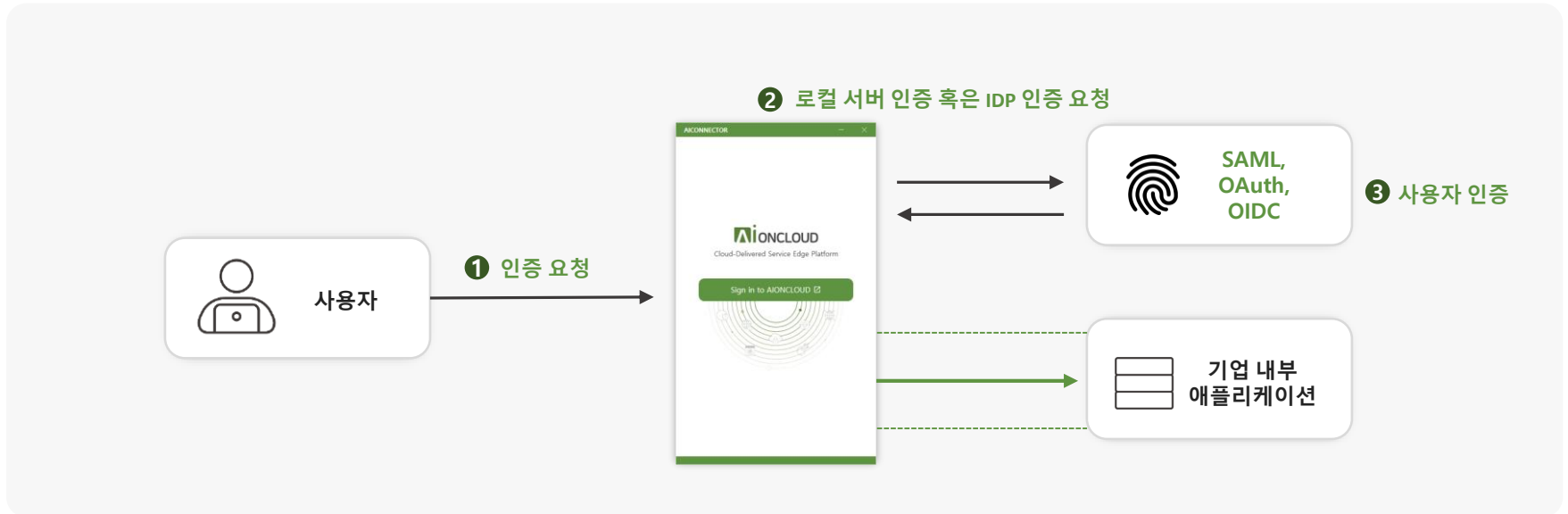


- **Active Directory Domain Joined** : 접속하려는 디바이스가 Active Directory에 등록되어 있는지 확인합니다.
- **Antivirus** : 특정 Antivirus가 실행 중인지 확인합니다.
- **Root CA Certificate** : 디바이스 내 인증서를 확인합니다.
- **File & Path** : 특정 파일의 유무 및 경로를 확인합니다.
- **Firewall** : 방화벽 실행 여부를 확인합니다.
- **Process Name** : 프로세스 이름을 확인합니다.
- **OS version & Patch** : OS 버전과 패치를 확인합니다.
- **Serial Number** : 디바이스의 시리얼 넘버를 확인합니다.

- 접근하려는 기기가 정해진 보안 정책(Device Posture)을 준수하는지 확인
- 기기의 상태나 보안 정책을 기반으로 접근을 허용하거나 차단하는 등 보다 정교한 보안을 제공

Features & Benefits

User authentication

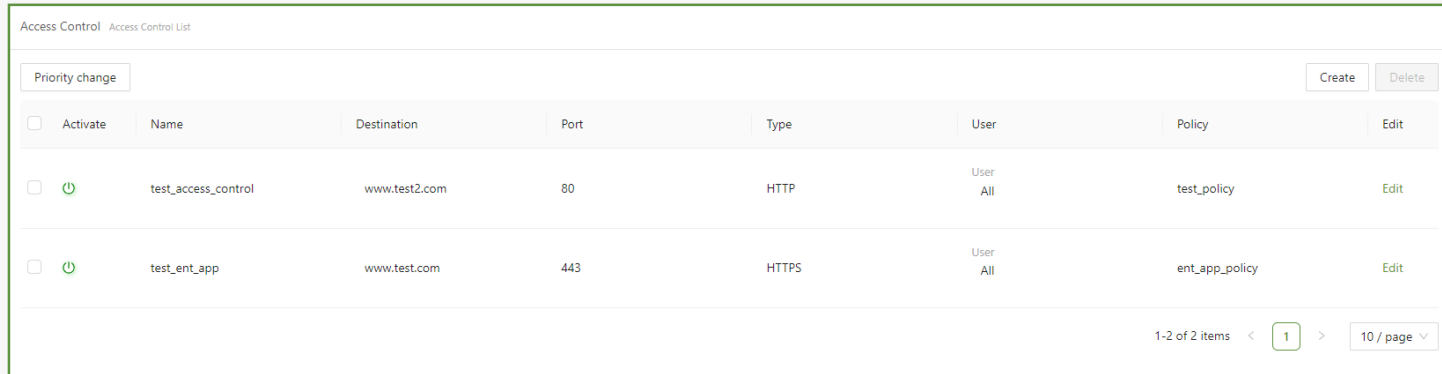


- 사용자 인증 통합을 통한 사용자 편의성, 강화된 보안, 관리 용이성, 쉬운 컴플라이언스 준수를 보장
- 기존 **사용자 인증 체계에 대한 완전한 유지 및 SSO(Single Sign-on)** 지원



지원 IDaaS: Okta, MS Entra ID(구 MS Azure AD)

Features & Benefits

User to app segmentation



The screenshot displays the 'Access Control' interface with a table of access control rules. The table has columns for 'Name', 'Destination', 'Port', 'Type', 'User', 'Policy', and 'Edit'. Two rules are listed: 'test_access_control' and 'test_ent_app'. Both rules are active, indicated by a green power icon. The 'test_access_control' rule has a destination of 'www.test2.com', port '80', and type 'HTTP'. The 'test_ent_app' rule has a destination of 'www.test.com', port '443', and type 'HTTPS'. Both rules are associated with 'User: All' and have their own policies: 'test_policy' and 'ent_app_policy' respectively. The interface also includes a 'Priority change' button, 'Create' and 'Delete' buttons, and a pagination bar showing '1-2 of 2 items' and '10 / page'.

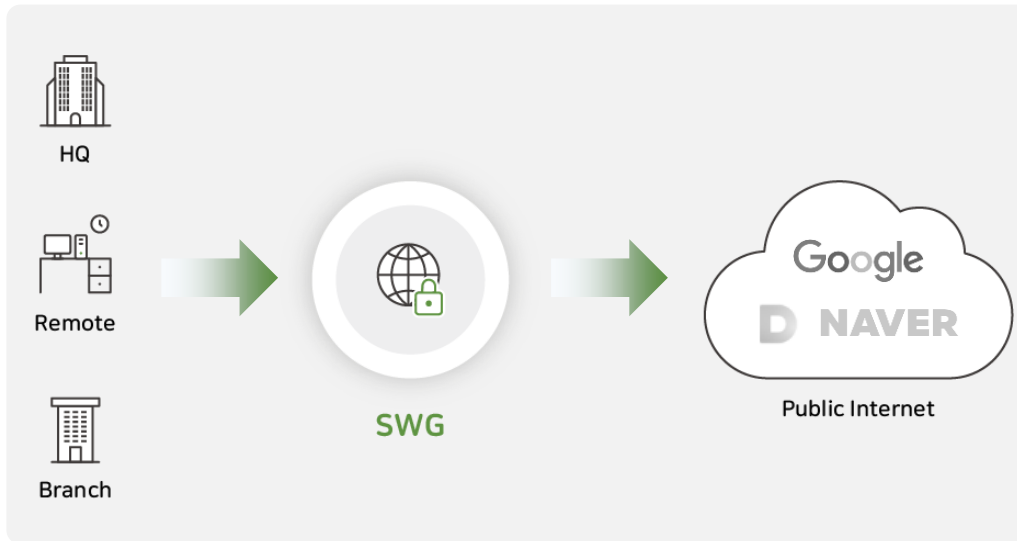
<input type="checkbox"/> Activate	Name	Destination	Port	Type	User	Policy	Edit
<input type="checkbox"/> 	test_access_control	www.test2.com	80	HTTP	User All	test_policy	Edit
<input type="checkbox"/> 	test_ent_app	www.test.com	443	HTTPS	User All	ent_app_policy	Edit

- 등록된 모든 프라이빗 애플리케이션이 **최소한의 권한으로 접근하도록 보장**
- 네트워크에 연결하지 않고 **사용자 to 애플리케이션 직접 연결**하여 보안 유지
- 사용자-애플리케이션 분할을 통해 오직 권한이 있는 사용자에게 **특정 애플리케이션에 대한 안전한 접근**을 제공
- 사용자, 접속시간, 접속위치, IP 주소 등 **컨텍스트 기반의 접근 정책** 설정

02

APPLICATION *i*NSIGHT SWG-RBI

SWG (Secure Web Gateway) Features & Benefits



Create Security Policy

Activate: ☐

Name:

Description:

Schedule: ☒ Unused ☐ Use One Time

Remote Browser: ☐ Untrusted ☐ Use P2P-RL

Block Page: DEFAULT

Action: ☒ Block ☐ Allow ☐ Logging

Member: Please check user or user group

User:

User Group:

Rule: Please create at least 1 rule.

Subject	Condition
<input type="checkbox"/> SaaS Category	in
<input type="checkbox"/> AND Anti-Virus	is
<input type="checkbox"/> AND HTTP Category	in

Enable

1-3 of 3 items

Cancel OK

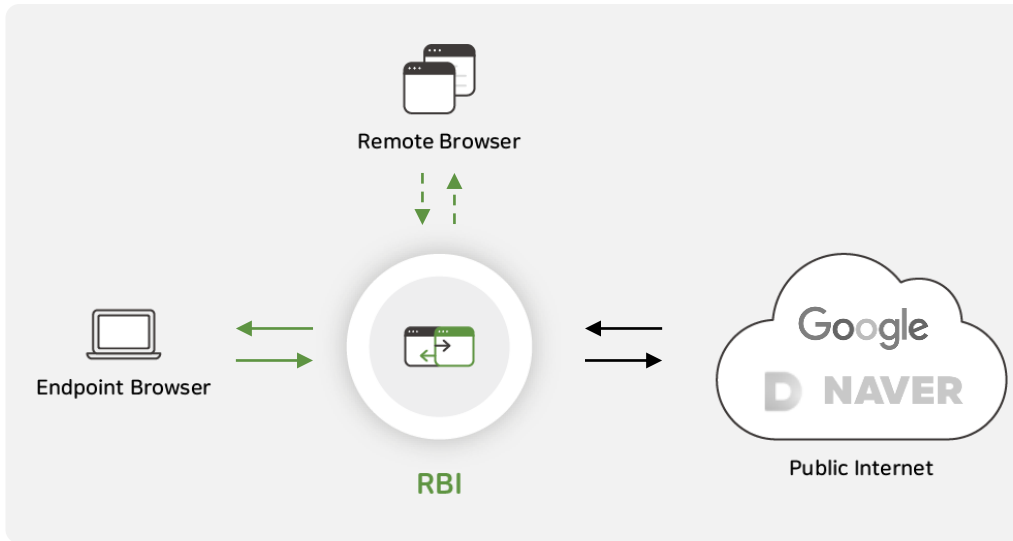
직원의 안전한 인터넷 사용

인터넷 구간 전역에 걸친 보안 제공

프록시로서 실시간 통신 트래픽 핸들링

SSL/TLS 복호화, URL 필터링, 안티멀웨어

RBI (Remote Browser Isolation) Features & Benefits



웹 브라우징 세션을 원격 서버에서 실행

직접적인 악성 코드에 노출되는 것을 방지

원격 렌더링 후 이미지/비디오 형식으로 전달

RBI 대상 보안 정책 적용 가능

THANK YOU