망분리 규제 완화,
보안 전략의 핵심은 ZTNA와 RBI

MONITORAPP | 박호철 수석연구원

망분리 규제 완화 & 제로 트러스트

MONITORAPP

망분리 규제?

외부 침입으로부터 내부 전산자원을 보호하기 위해 내부망과 외부망을 분리하는 네트워크 보안 정책

- 2006년 국가 및 공공 기관 우선 도입
- 2013년 대규모 금융 전산 사고를 계기로 금융권 확산

망분리 규제 완화 & 제로 트러스트

MONITORAPP

보안 강화를 위한
물리적 망분리

내부망(업무망)

금융 및 공공 기관

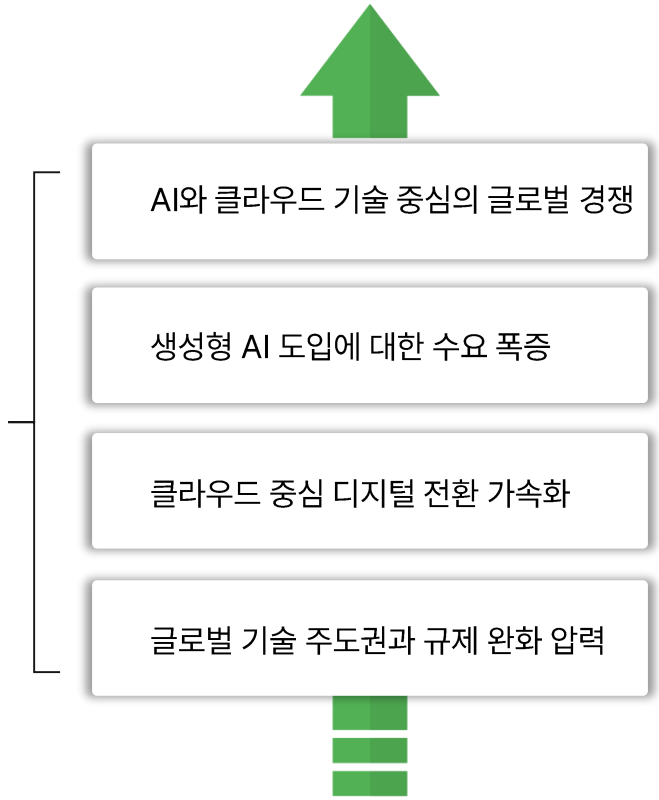
외부망(인터넷망)

물리적 망분리

망분리 규제 완화 & 제로 트러스트

클라우드 전환과
AI 플랫폼 사용 증가

물리적 · 논리적 망분리



망분리 규제 완화 & 제로 트러스트

MONITORAPP

혁신 & 보안의 균형을 위한 점진적인 규제 개선

⚠ 논리적 망분리 기반 데이터 중요도 중심의 차등 적용

- 기밀 : 엄격 통제(Classified)
- 민감 : 제한 접근(Sensitive)
- 공개 : 활용우선(Open)

제로 트러스트 도입이 필수

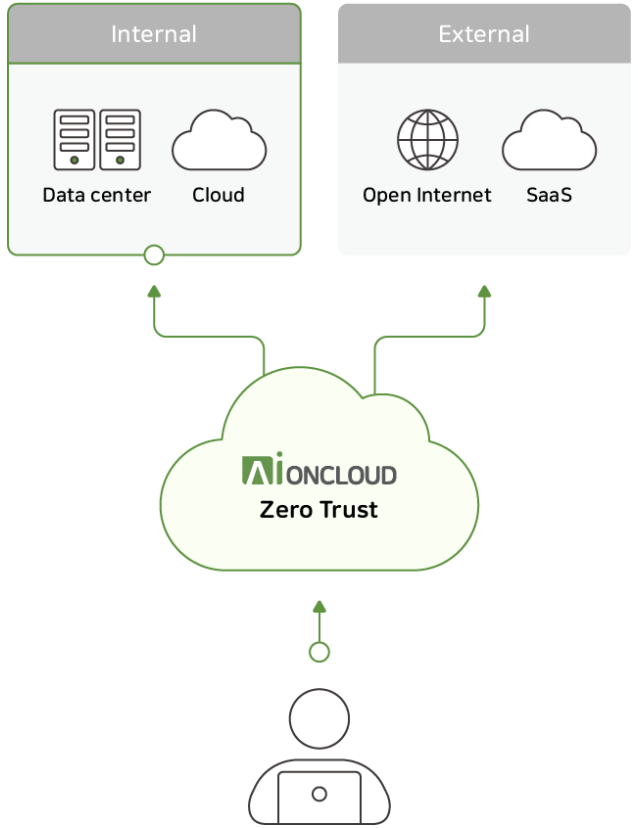
- 인터넷 단말의 업무 효율성 제고
- 업무환경에서 생성형 AI 활용
- 외부 클라우드 활용한 업무협업 체계
- 업무 단말의 인터넷 이용
- 공공 데이터의 외부 AI 융합
- 연구목적 단말의 신기술 활용
- 개발 환경 편의성 향상
- 클라우드 기반 통합 문서 체계

어디서든 공통된 보안과 통제

MONITORAPP

내부와 외부를 구분하지 않고, 신뢰하지 않고 항상 확인한다.

- 디지털 전환 환경에 적합한 SaaS 활용 증가 예상
- 서비스 프로덕션 환경의 멀티·하이브리드 클라우드화
- 변화하는 디지털 환경에 적합한 새로운 보안 전략의 도입이 필수



Zero Trust Network Access

MONITORAPP

어떻게 하면 제로 트러스트 원칙 기반하에

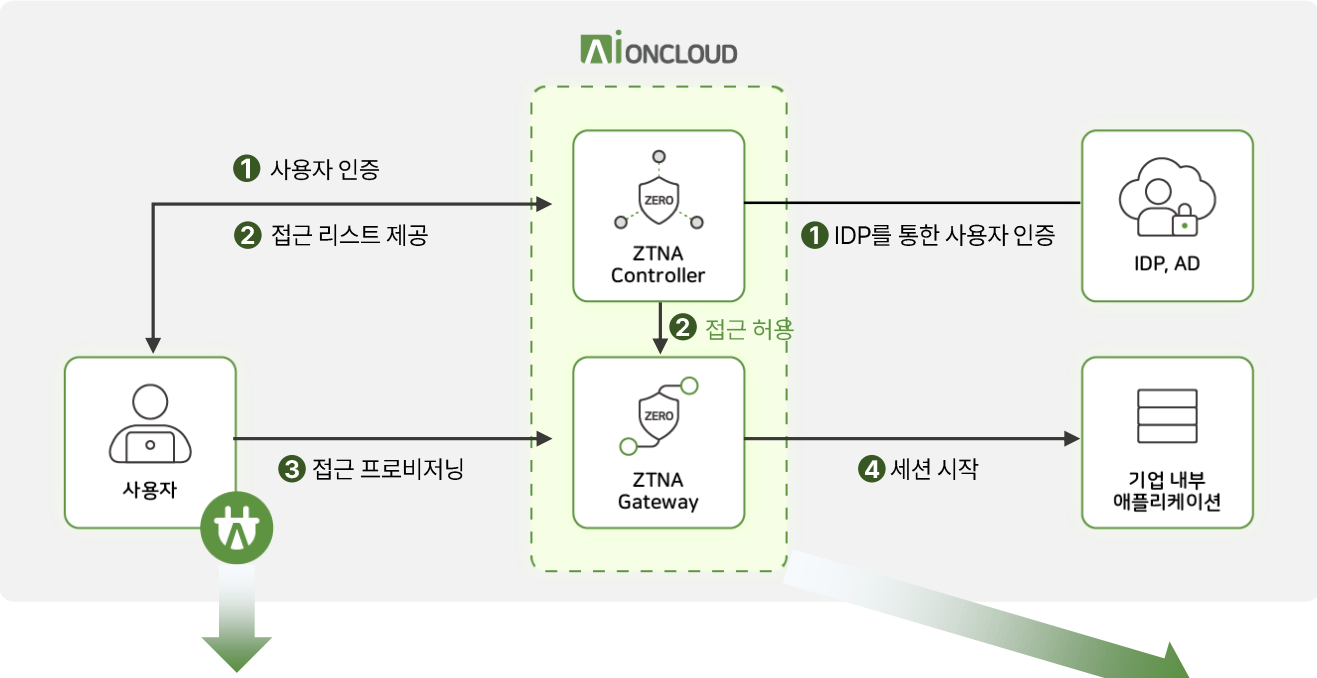
"기업 애플리케이션" 을 이용할 수 있을까 ?

ZTNA Vs SSL VPN

MONITORAPP

항목	ZTNA (SDP Framework)	SSL VPN
보안 접근 방식	**최소 권한 원칙 (Least Privilege) 기반**	네트워크 전체 접근 허용 (All-or-Nothing)
접근 방식	**애플리케이션 단위 접근 제어 (Micro-Segmentation)**	네트워크 단위 접근 제어
보안 리스크	**디바이스 신뢰성 평가 후 접근 허용(Device Posture Check)**	VPN 연결 시 내부 네트워크 노출 가능
확장성	클라우드·온프레미스 혼합 환경 최적화	온프레미스 중심, 클라우드 확장 어려움
규제 대응	망분리 규제 완화(N2SF) 환경에 적합	망분리 환경에서 관리 복잡성 증가
인증	**MFA 및 컨텍스트 기반 인증(FIDO, Step-up Auth 등)**	단일 사용자 인증
사용 사례	원격 근무, 제로 트러스트 보안, B2B 협업	내부 네트워크 접근, 전통적인 원격 접속

ZTNA : 안전한 기업 리소스 접근



- SSO, 로컬 DB를 통한 사용자 인증(컨텍스트 분석)
- 컨텍스트 기반 보안 정책 적용
- 정책에 따른 터널링 구현, 마이크로 세그먼테이션 적용

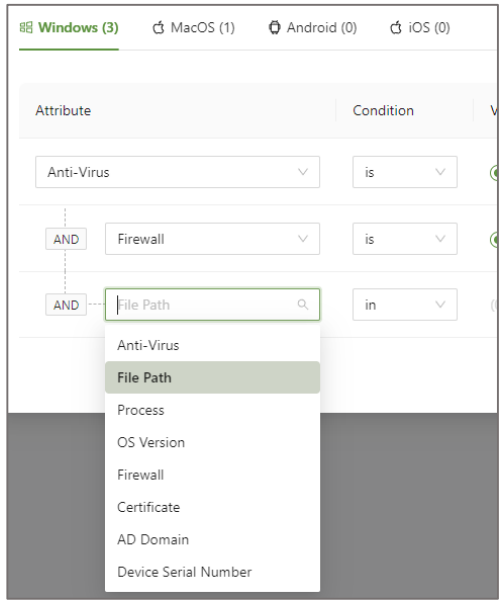
End-point Device Posture Check

- 접근 기기가 정해진 보안 정책(Device Posture)을 준수하는지 확인
- 기기의 상태나 보안 정책을 기반으로 접근 허용, 차단하여 보다 정교한 보안 제공
- 프로세스, 방화벽, 파일 경로, OS 버전, 시리얼 번호, 인증서, 안티바이러스 등

User to App Segmentation

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

ZTNA : 안전한 기업 리소스 접근



DPC Attribute

안티바이러스

파일 경로

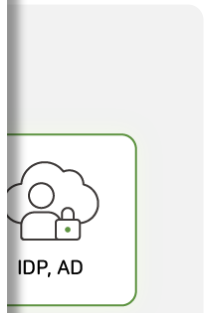
디바이스 OS 버전

방화벽

인증서

디바이스 시리얼 넘버

EDR 점수



- SSO, 로컬 DB를 통한 사용자 인증(컨텍스트 분석)
- 컨텍스트 기반 보안 정책 적용
- 정책에 따른 터널링 구현, 마이크로 세그먼테이션 적용

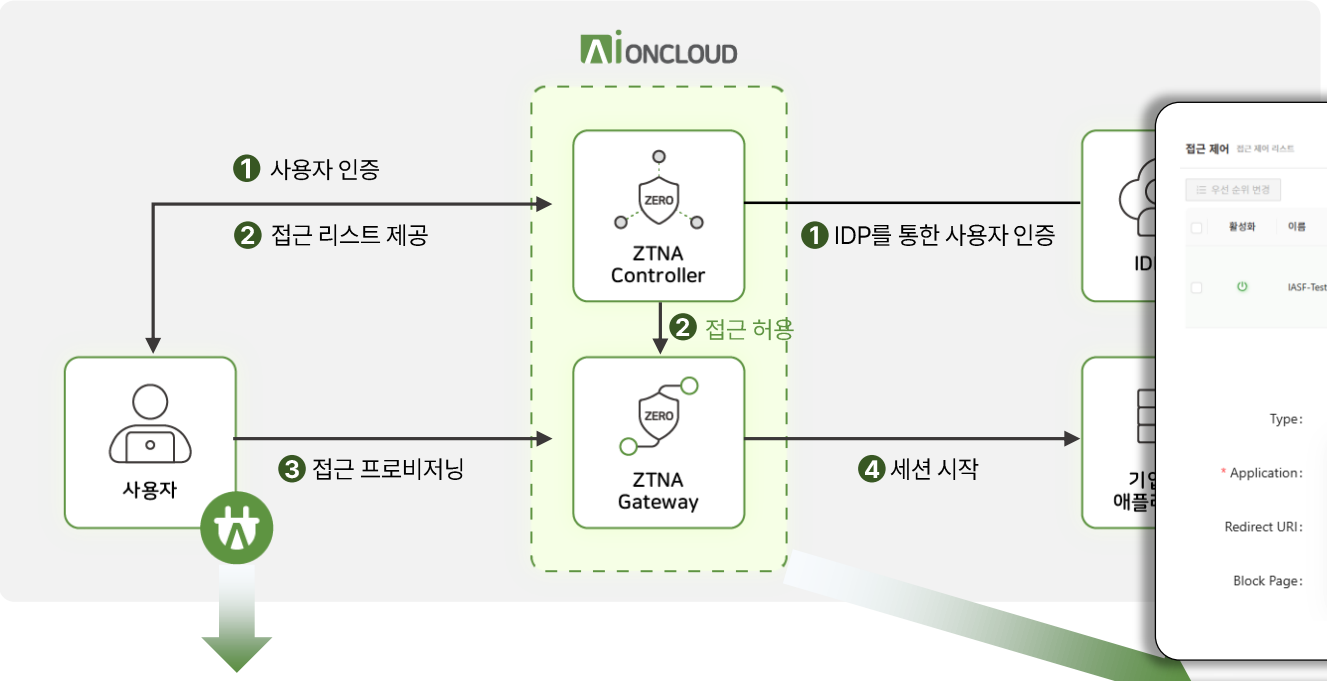
End-point Device Posture Check

- 접근 기기가 정해진 보안 정책(Device Posture)을 준수하는지 확인
- 기기의 상태나 보안 정책을 기반으로 접근 허용, 차단하여 보다 정교한 보안 제공
- 프로세스, 방화벽, 파일 경로, OS 버전, 시리얼 번호, 인증서, 안티바이러스 등

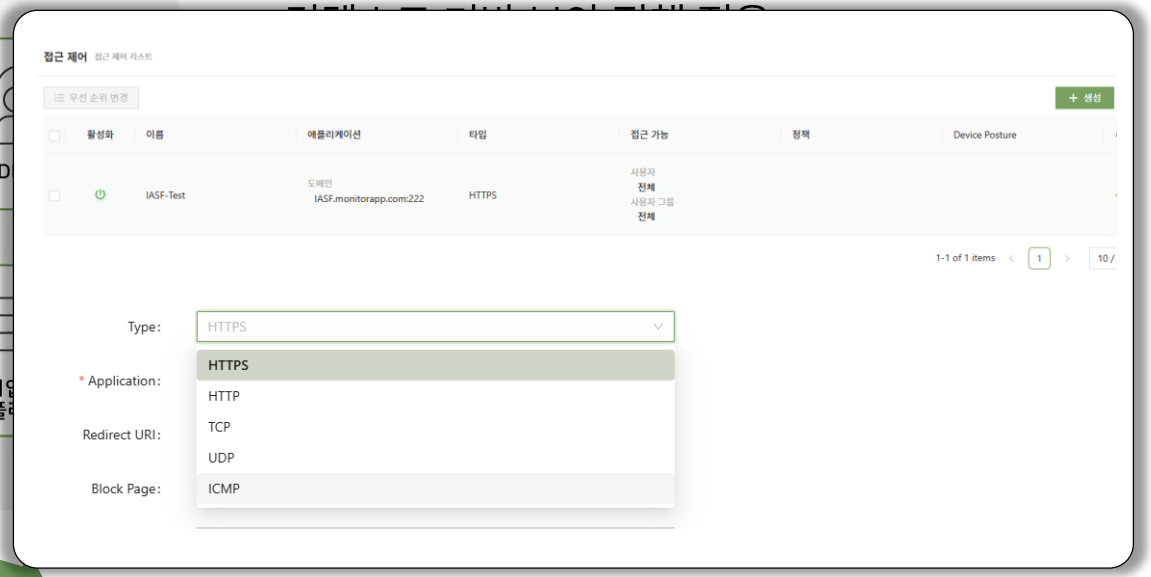
User to App Segmentation

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

ZTNA : 안전한 기업 리소스 접근



- SSO, 로컬 DB를 통한 사용자 인증(컨텍스트 분석)



End-point Device Posture Check

- 접근 기기가 정해진 보안 정책(Device Posture)을 준수하는지 확인
- 기기의 상태나 보안 정책을 기반으로 접근 허용, 차단하여 보다 정교한 보안 제공
- 프로세스, 방화벽, 파일 경로, OS 버전, 시리얼 번호, 인증서, 안티바이러스 등

User to App Segmentation

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

모니터랩의 ZTNA

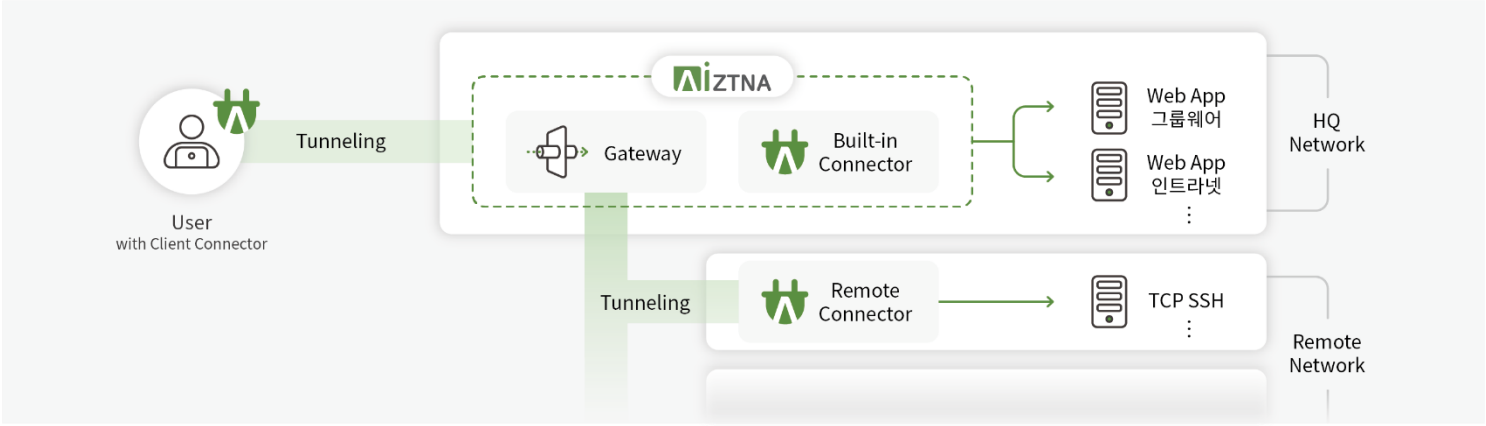
MONITORAPP

AIONCLOUD SRA

SaaS 기반의 ZTNA

AIZTNA

온프레미즈 기반의 ZTNA



Remote Browser Access

MONITORAPP

어떻게 하면 제로 트러스트 원칙 기반하에

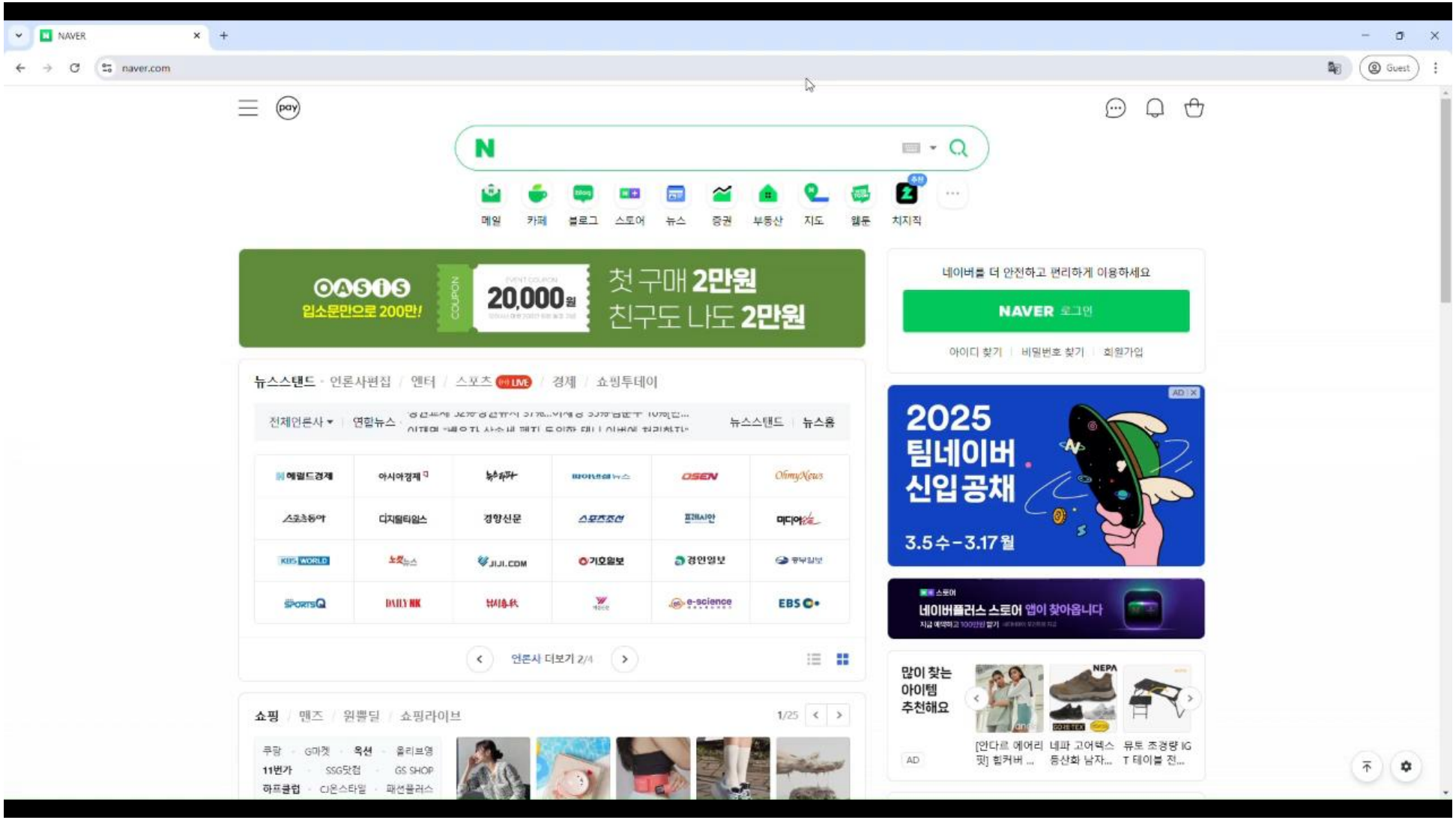
“SaaS 애플리케이션” 을 이용할 수 있을까 ?

VDI와 RBI

	VDI	RBI
격리 방식	원격 가상 데스크톱에서 전체 환경 실행	원격 가상 브라우저에서 웹 콘텐츠 실행
보안 모델	전체 OS 및 애플리케이션 격리	웹 및 브라우저 기반 서비스스만 격리
운영 및 유지보수	고비용, 복잡한 인프라 및 유지보수 필요	VDI 대비 저비용, 운영 부담 적음.
네트워크 부하	높음 (전체 데스크톱 스트리밍 필요)	낮음 (웹 콘텐츠만 스트리밍)
적합한 환경	내부 애플리케이션 사용이 많은 환경	웹 기반 업무 환경 및 SaaS, 클라우드 기반 업무

망분리 규제 완화 이후 SaaS와 클라우드 중심의 업무 환경으로 전환하는 기업이라면, VDI 대비 RBI가 합리적인 솔루션

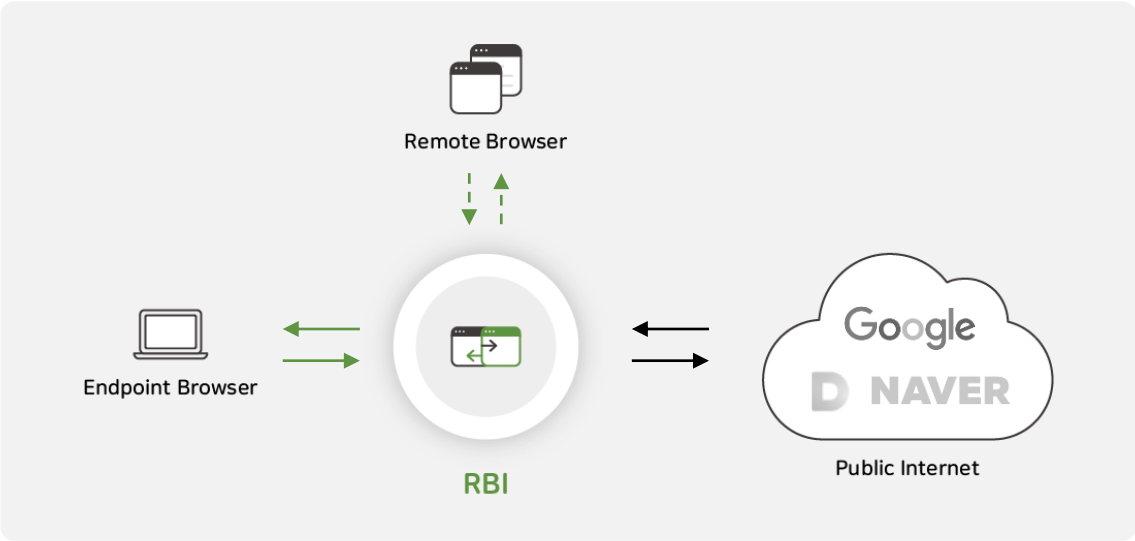
RBI 시연 (영상)


NAVER
naver.com
Guest
pay
N
메일
카페
블로그
스토어
뉴스
증권
부동산
지도
웹툰
치지직
OASIS
입소문만으로 200만!
COUPON
20,000원
첫 구매 2만원
친구도 나도 2만원
네이버를 더 안전하고 편리하게 이용하세요
NAVER 로그인
아이디 찾기 | 비밀번호 찾기 | 회원가입
뉴스스탠드 · 언론사편집 / 엔터 / 스포츠 LIVE / 경제 / 쇼핑투데이
전체언론사 | 연합뉴스
뉴스스탠드 | 뉴스홈
언론사 더보기 2/4
2025
팀네이버
신입공채
3.5수-3.17월
AD
네이버플러스 스토어 앱이 찾아옵니다
많이 찾는
아이템
추천해요
AD
쇼핑 / 맨즈 / 원쁠딜 / 쇼핑라이브
1/25
쿠팡 · G마켓 · 옥션 · 올리브영
11번가 · SSG닷컴 · GS SHOP
하프클럽 · 디온스타일 · 패션플러스

RBI: 원격 브라우징 솔루션

✓망분리 규제 완화에 따른 필수 보안 서비스

- 웹 브라우징을 원격 서버에서 실행
- 직접적인 악성 코드에 노출되는 것을 방지
- 원격 렌더링 후 이미지/비디오를 사용자 브라우저로 전달
- 원격 브라우저 트래픽도 보안 정책 적용 (SWG, CASB 정책 적용)



RBI: 완전한 브라우저 격리

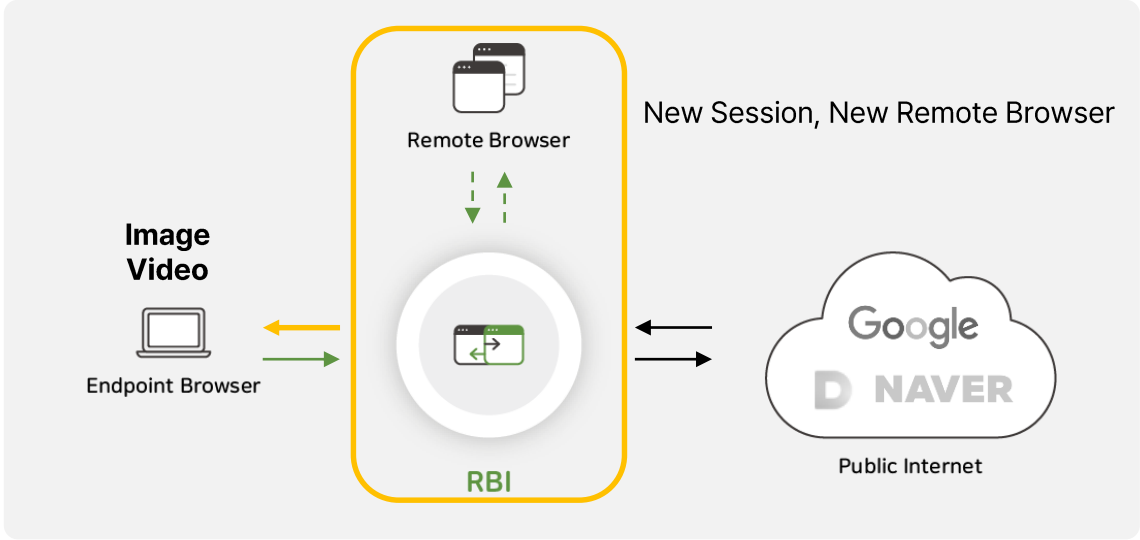
- 완전 격리된 원격 브라우저가 웹 사이트 방문

  → 사용자 보안 정책에 따른 RBI 적용 대상 웹사이트

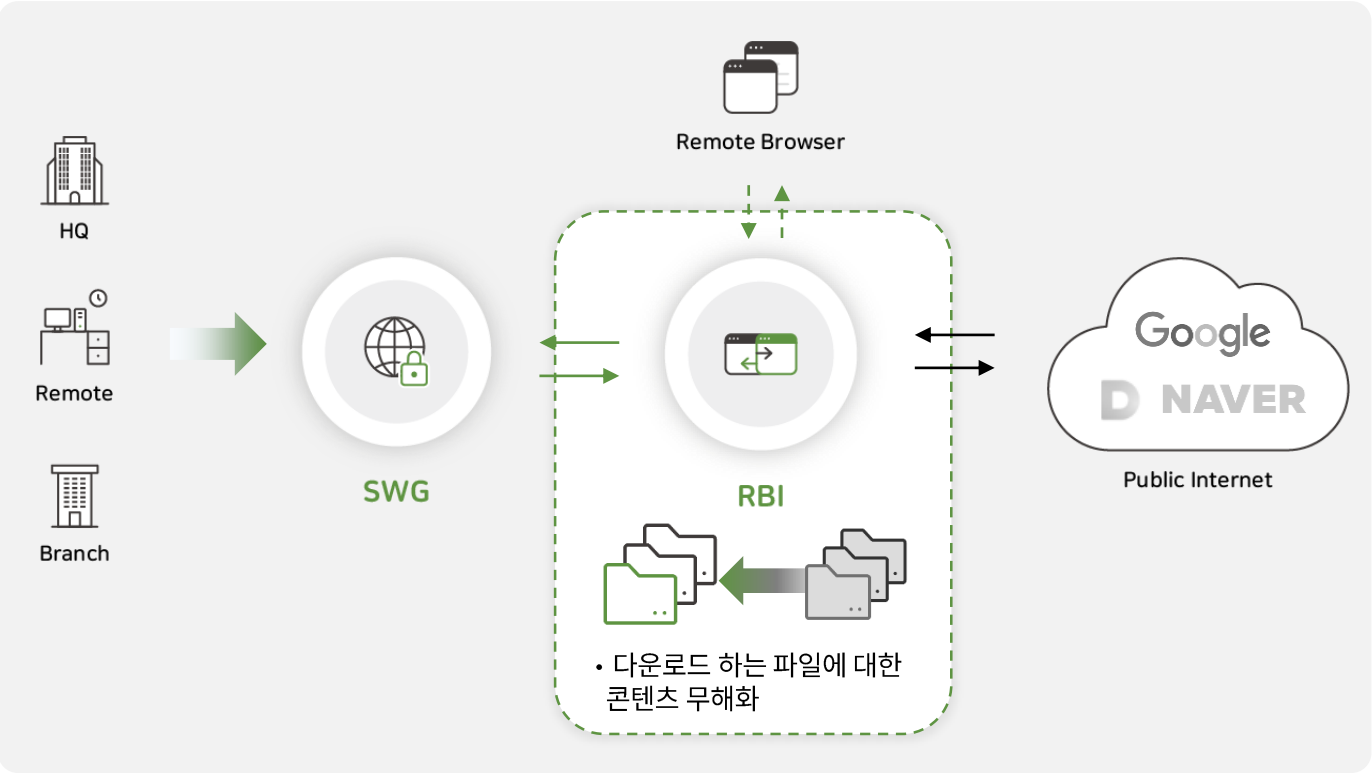
- 오직 실행된 결과값만을 렌더링하여 사용자 브라우저에 전달

  → 이미지/비디오 스트리밍 방식으로 이질감 없는 웹브라우징

- 악성 웹사이트에 접속하거나 악성 스크립트가 포함된 페이지를 로드 하더라도, 감염된 가상 브라우저는 타임아웃 이후 자동 폐기

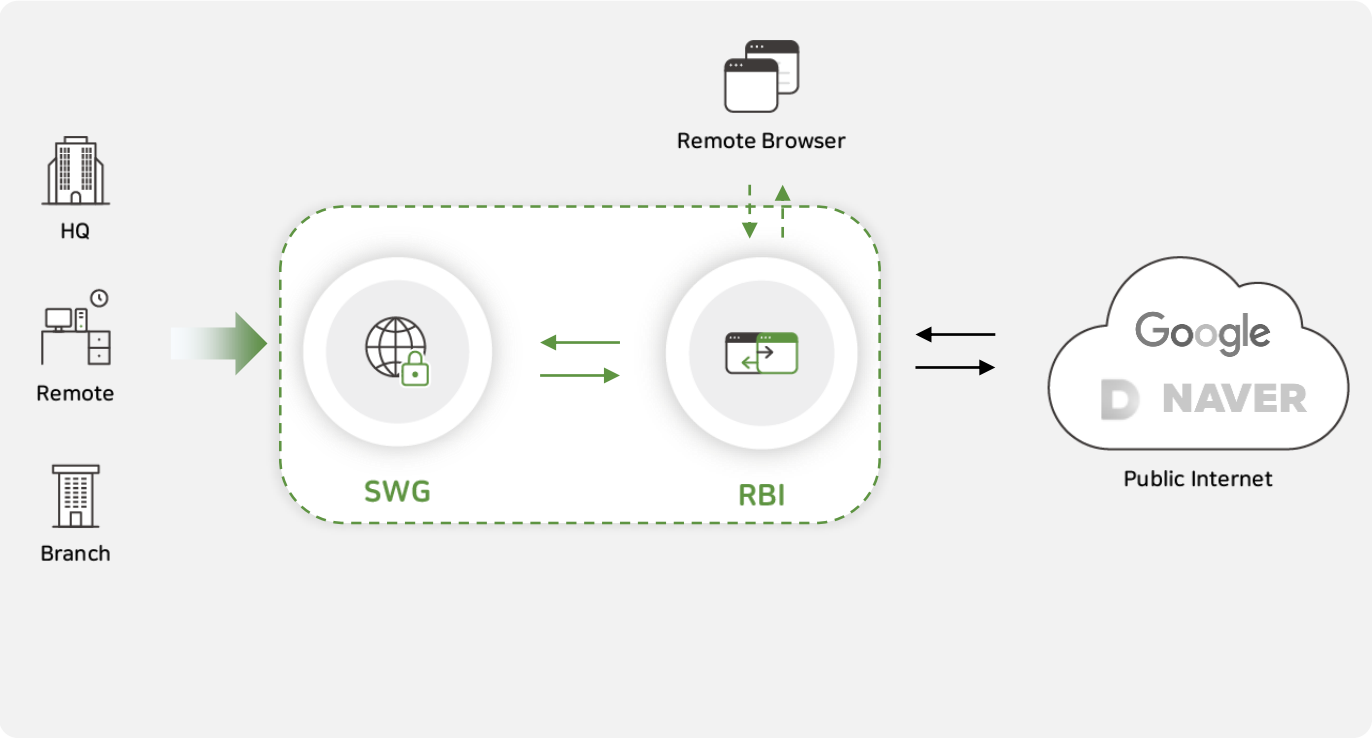


RBI: 콘텐츠 무해화(CDR)



- Type1. PDF 파일로 변경후 전송
- Type2. 문서 내 실행 콘텐츠 제거후 전송

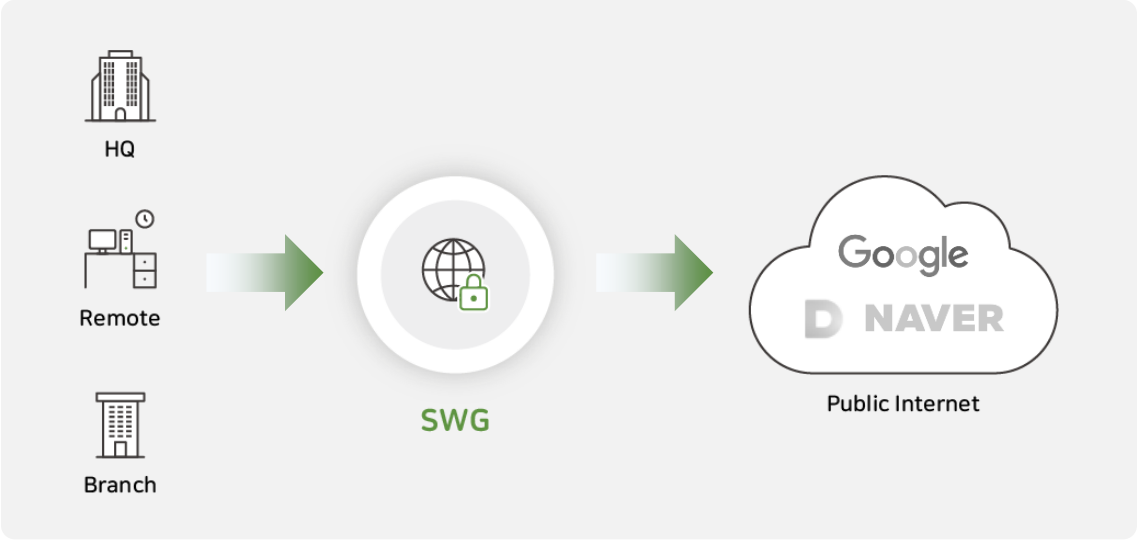
RBI: SWG·CASB와 함께 강력해진 보안



- RBI는 악성 코드 감염을 원천 차단하는 역할
- SWG는 접근 제어, 파일 보안, 트래픽 가시성과 같은 보안 기능 수행

SWG: 사용자의 안전한 웹 환경 제공

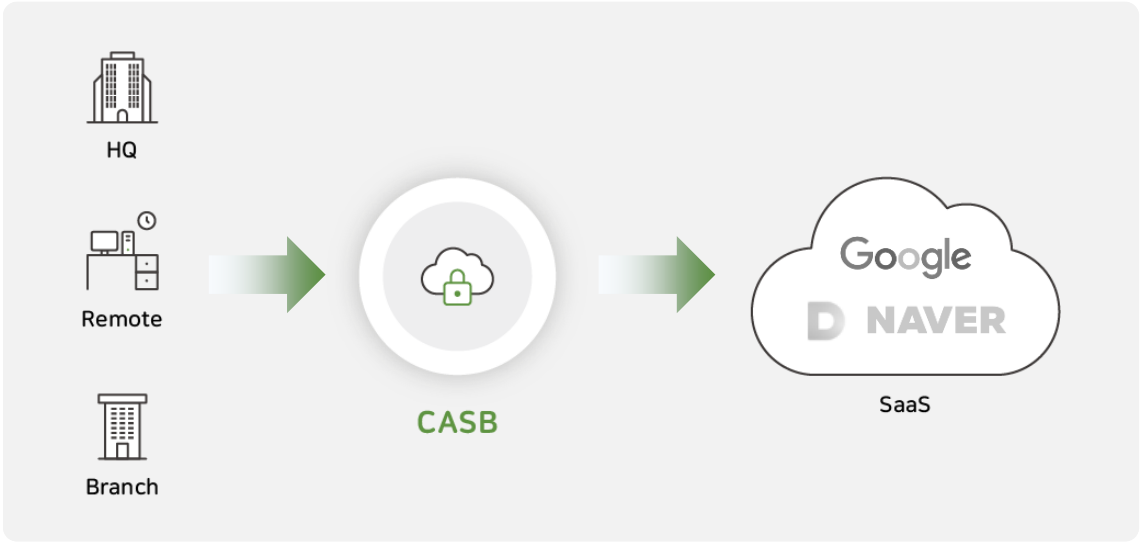
- 직원의 안전한 인터넷 사용
- 인터넷 구간 전역에 걸친 보안 제공
- 프록시 형태로 실시간 통신 트래픽 제어
- SSL/TLS 복호화, URL 필터링, 안티멀웨어



CASB: 안전한 SaaS 사용 환경 제공

MONITORAPP

- 기업에서 인가한 SaaS 기능 제어 및 모니터링
- API를 활용한 사후 모니터링 수행
- 비인가 SaaS (Shadow IT) 제어
- 적응형 기능 제어, SaaS 애플리케이션 가시성, 데이터 보안



CASB: 인라인 & API

MONITORAPP

Forward / Reverse

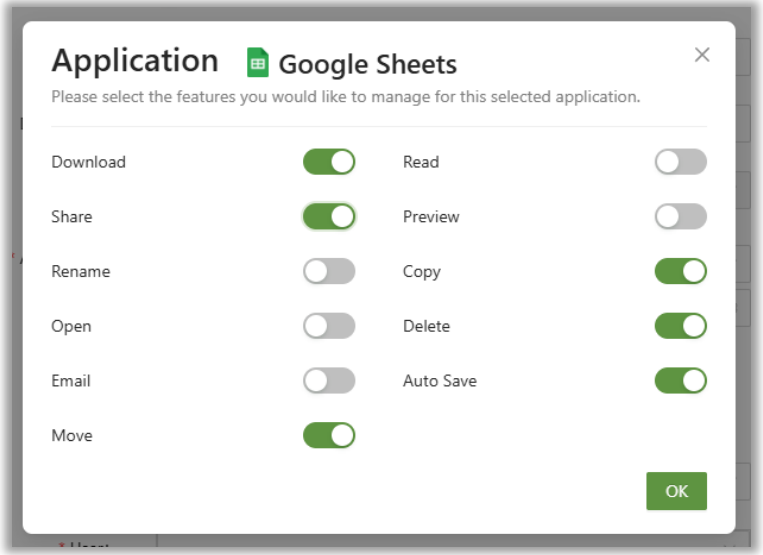
- 각 SaaS 애플리케이션의 고유한 기능을 제어(다운로드, 공유, 미리보기 등)
- SSO 통합으로 어디서 어떤 기기로 SaaS 접근하더라도 통제 가능

Ex)
Office 365 엑셀에서 영업팀의 읽기 허용, 복사, 프린트, 내보내기 금지

API

- 사후 모니터링 수행
- SaaS 애플리케이션 내부의 메타데이터 접근

Ex)
특정 사용자의 Salesforce 로그인 및 로그아웃 시간,
OneDrive에서 파일 업로드 및 다운로드 내역 등



모니터랩의 SWG · CASB · RBI

MONITORAPP

AIONCLOUD SIA

SaaS 기반의 SWG · CASB · RBI

AISWG with RBI

온프레미즈 기반의 SWG · CASB · RBI

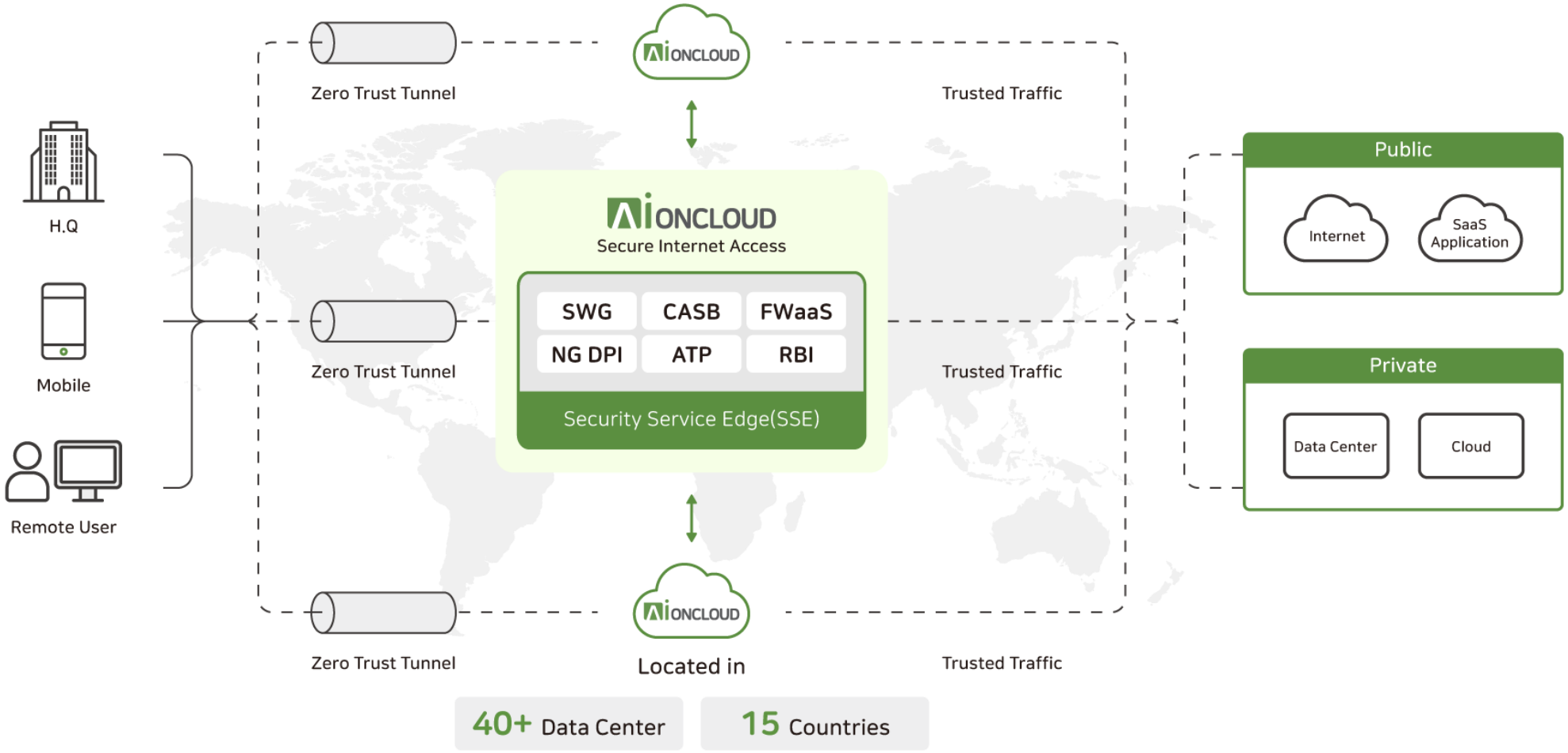
AISWG 피지컬 어플라이언스형

On-premise 환경에 최적화된 하드웨어 기반의 시큐어 웹 게이트웨이

RBI 피지컬 어플라이언스형

시큐어 웹 게이트웨이와 통합되는 하드웨어 기반의 원격 브라우저 격리

AIONCLOUD Security Service Edge Platform



감사합니다.