Application Delivery Leader
MONITORAPP

PASCON 2022
2022 공공 · 금융 · 기업 정보보안&개인정보보호 컨퍼런스

SASE 기반의 차세대 클라우드 보안

- 제로 트러스트와 SASE
- 안전한 원격근무를 위한 SSE

(주)모니터랩
박 호 철

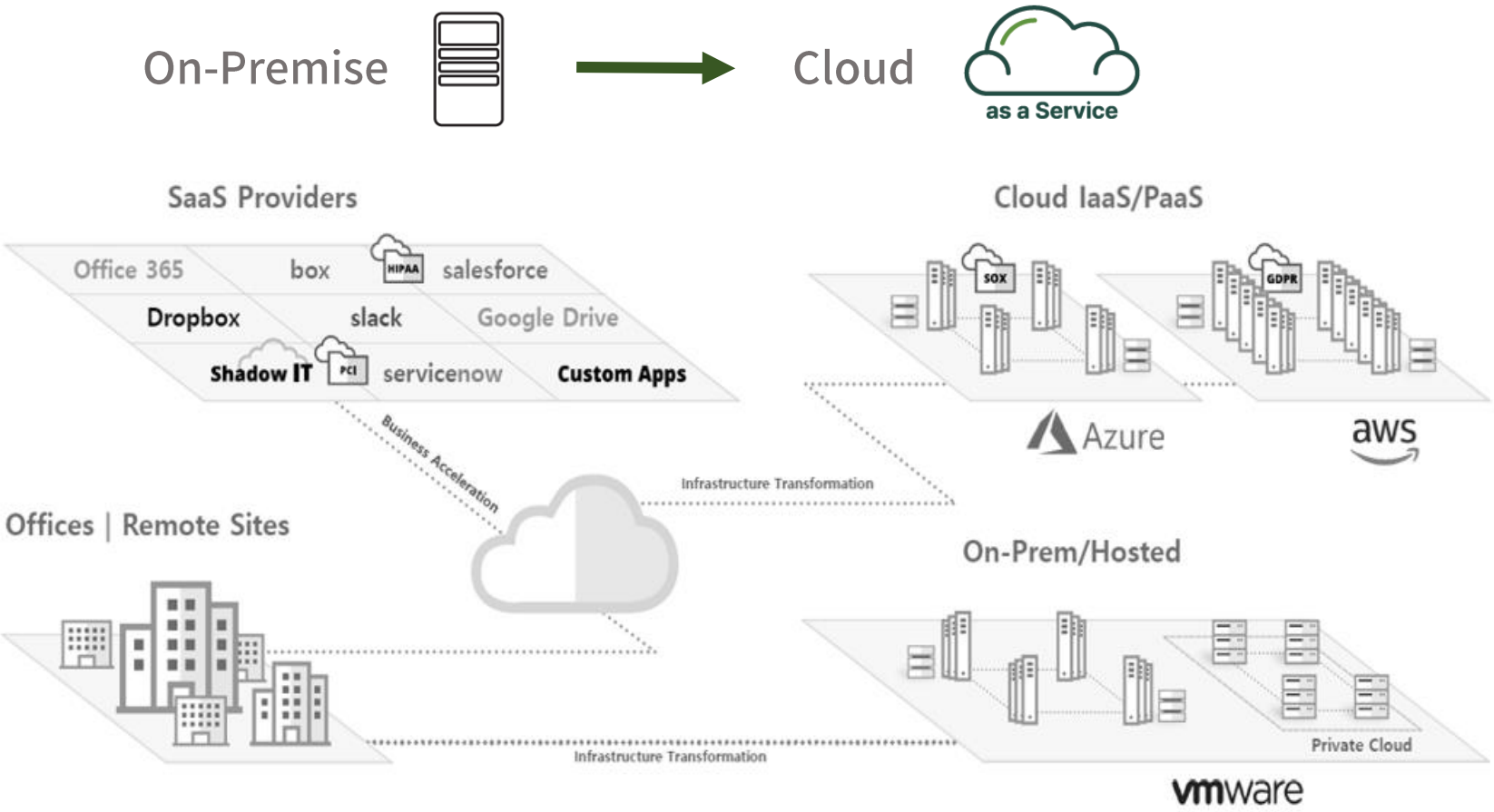
MONITORAPP

Application Delivery Leader
MONITORAPP

Contents

01. Zero Trust & SASE

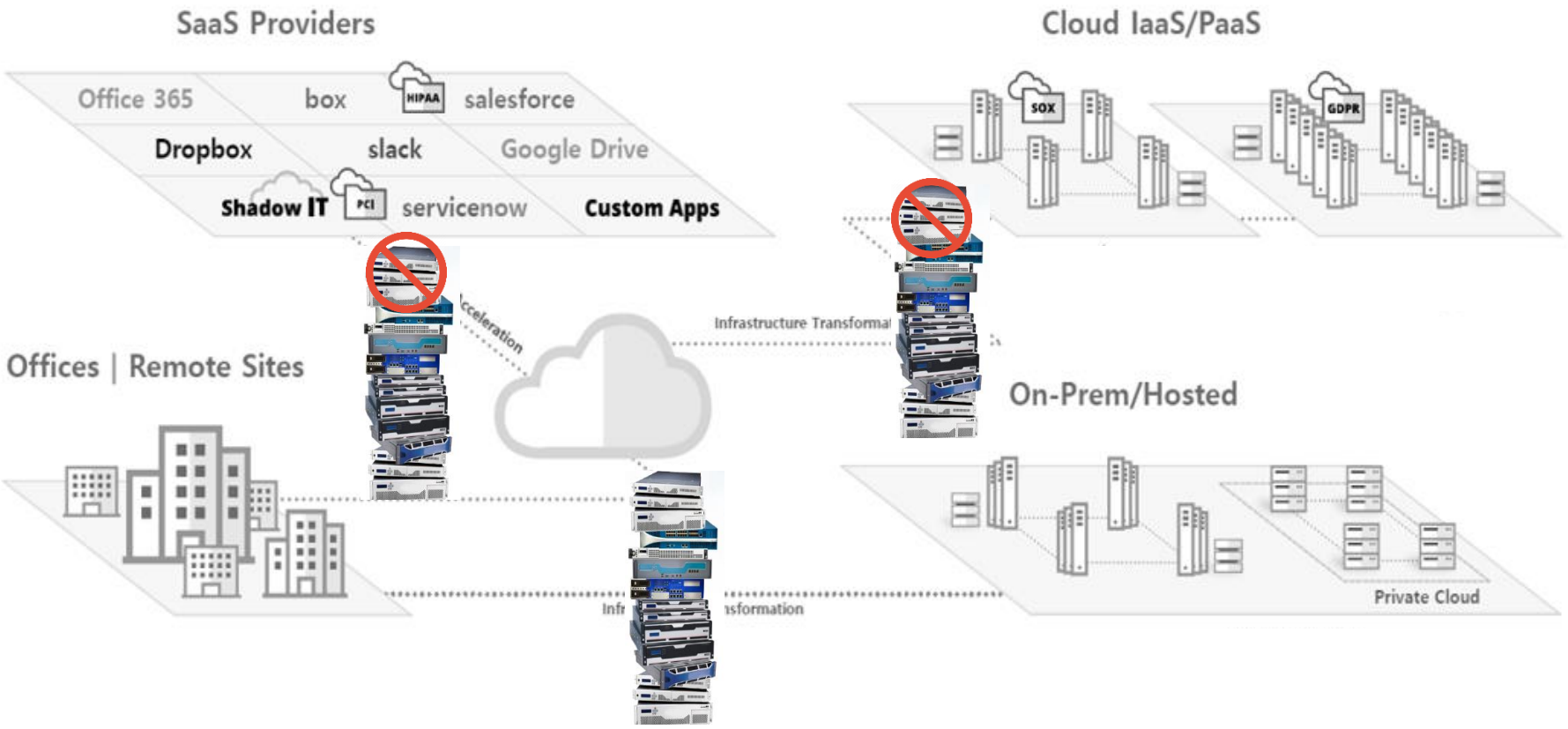
❖ 기업 IT 환경 변화



Cloud는 선택이 아닌 필수이며, **Cloud 전환에 보안은 가장 큰 고려 요소**

Application Delivery Leader MONITORAPP

❖ 기업 IT 환경 변화



본사/지사 환경과 On-Prem / IaaS / SaaS 이용 증가로 보안 환경 변화

기존 경계선 보안만으로는 한계

❖ Covid19로 인한 사무환경 변화와 보안위협 증가

위험도가 높은 APP과 웹사이트 접근이 Covid19 이전에 비해 161% 증가...

전체 인원의 **64%** 가 원격근무중

148% Covid19 이전에 비해 증가

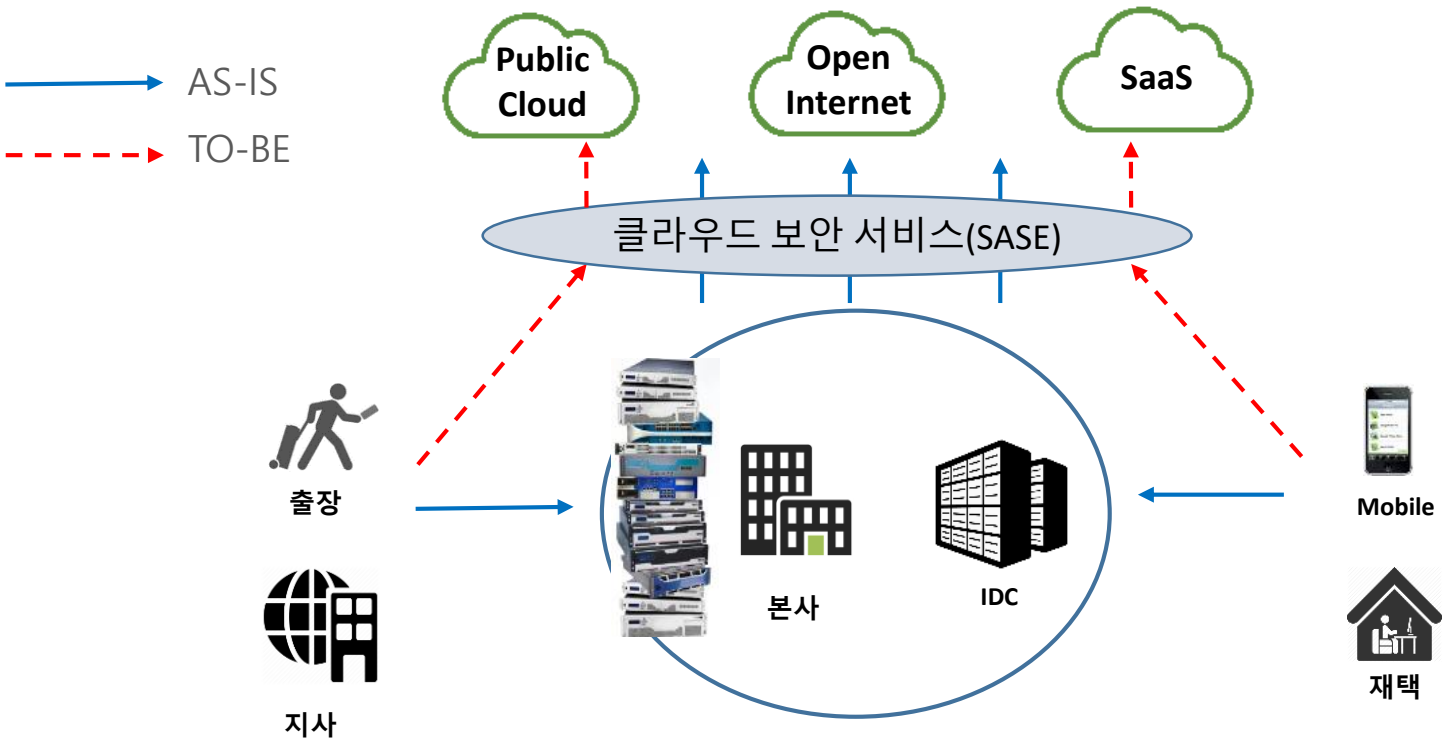
업무용 Device 개인용도 사용율 **97%**

80% 기업용 협업툴 사용율

-TechTarget 2020

Application Delivery Leader MONITORAPP

❖ Zero Trust

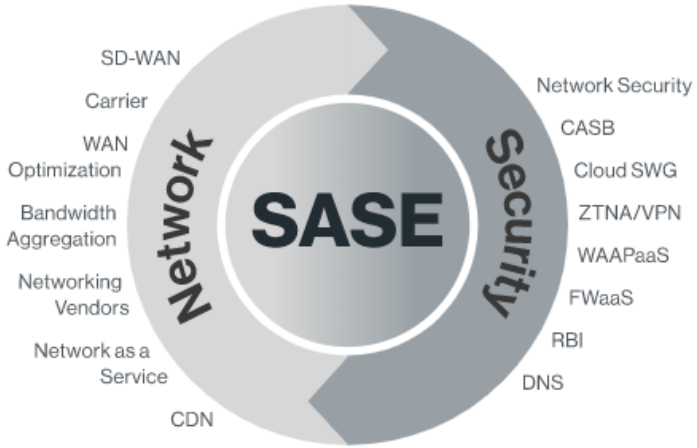


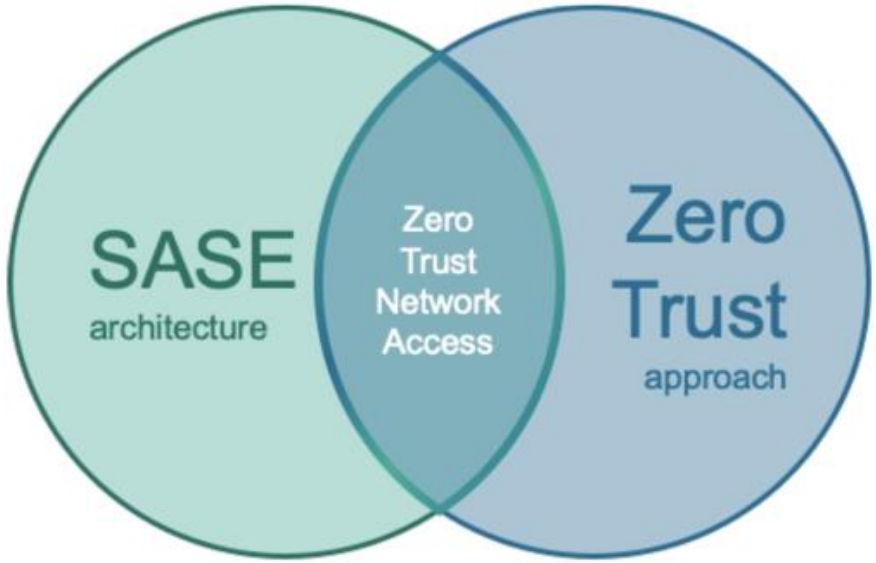
- 전통적인 경계선 보안
- DMZ / VPN …
- 네트워크 기반의 과도한 묵시적 신뢰

- **제로 트러스트**
- **ZTNA / SASE … ID&Context**
- **애플리케이션별 최소한의 권한 제공**

❖ SASE(Secure Access Service Edge)

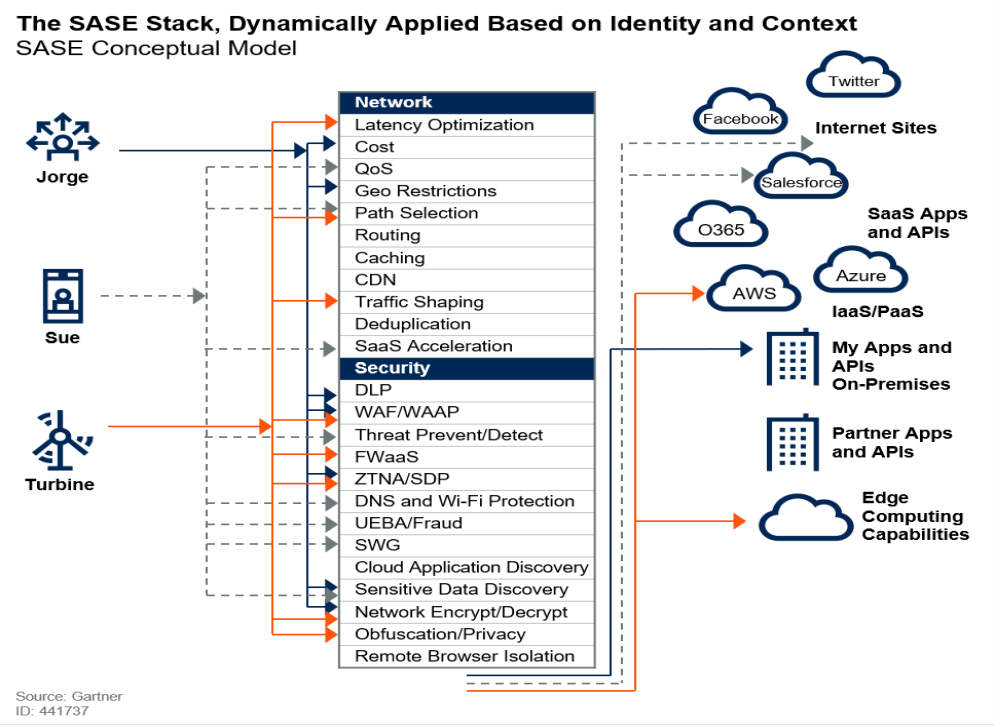
- SASE는 클라우드와 식별된 사용자 신원 기반의 네트워킹/보안 통합 아키텍처
- SASE를 통해 Security Anywhere 서비스 가능
- Zero Trust 원칙을 적용하기 위한 플랫폼





❖ SASE(Secure Access Service Edge)

- 네트워크 중심 → 사용자 중심으로
- 네트워크 보안 → 사용자 보안
- 보안기능 중심 → 정책관리 중심
- 보안 장비 별 관리 → 서비스 및 정책 통합관리



❖ SASE Vs SSE(Security Service Edge)

- SASE에서 SD-WAN을 제외한 보안 번들 : "보안 간소화"
- SSE는 완전한 SASE 채택을 위한 진입점 또는 첫 번째 단계 역할
- SASE는 온프레미스와 클라우드가 공존하는 상황에 초점
- SSE는 기업들의 클라우드 기반 원격 근무 중심에 초점

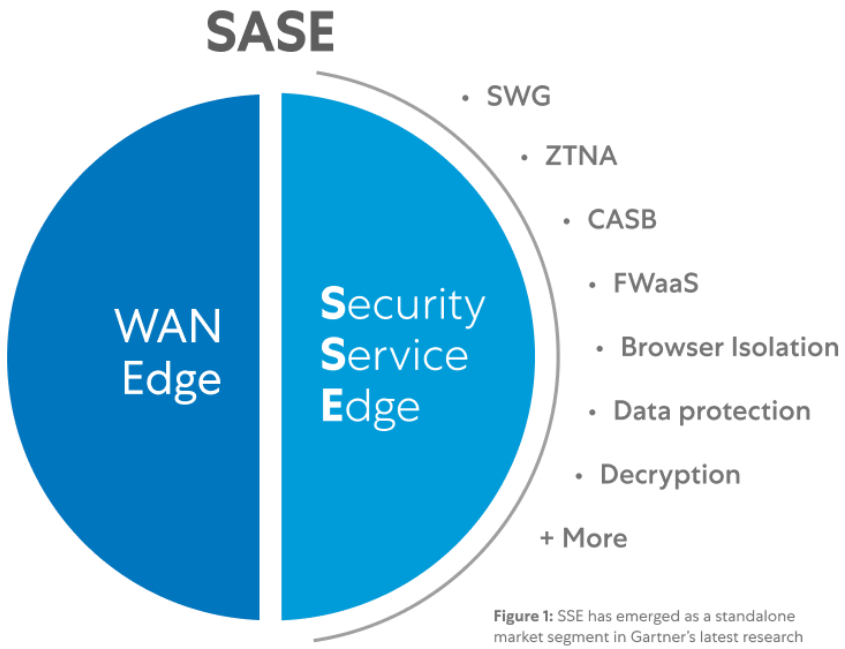
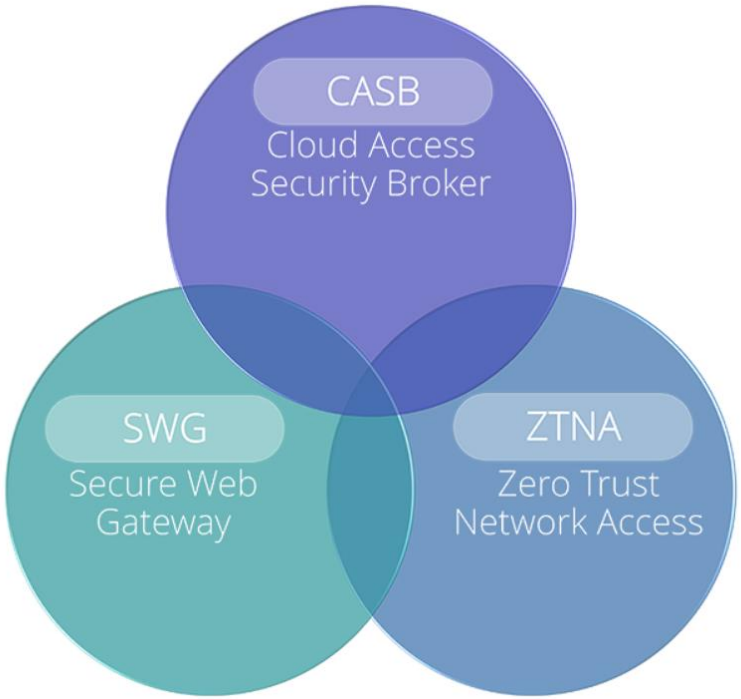


Figure 1: SSE has emerged as a standalone market segment in Gartner's latest research

❖ SSE(Security Service Edge)

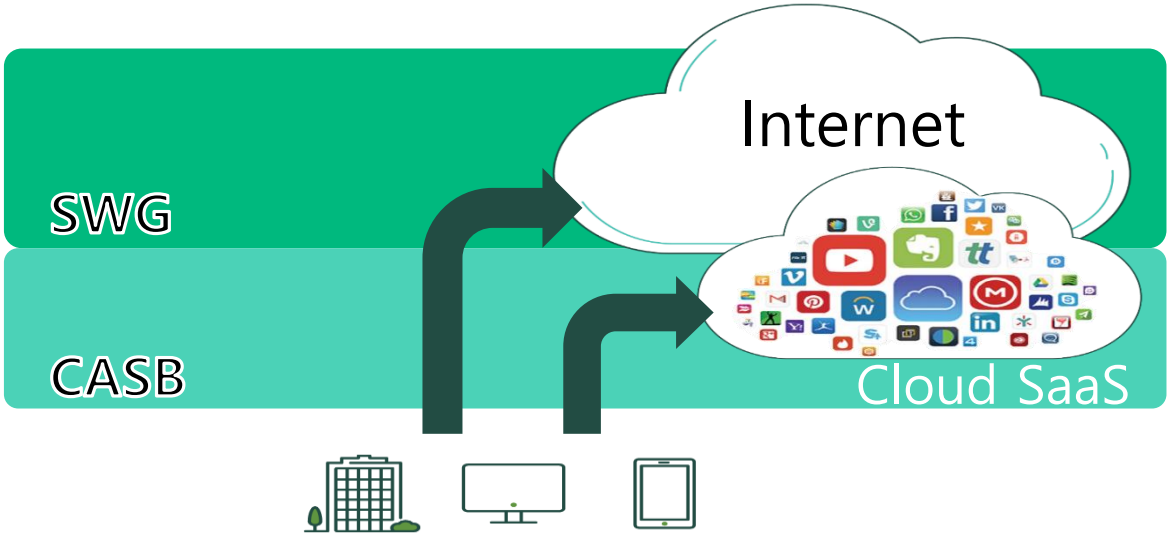
- SWG : 웹 요청을 기업 정책과 비교하여 위험한 프로그램과 웹사이트 접근 제한
- CASB : 직원을 Office 365 및 Salesforce와 같은 SaaS 애플리케이션에 연결
- ZTNA : 직원을 온프레미스 데이터 센터 또는 클라우드에서 실행되는 기업 애플리케이션에 연결



❖ SWG Vs CASB

- SWG(Secure Web Gateway)
  : 안전한 인터넷 사용에 초점 (세분화 된 SaaS 보호 기능 없음)
  : URL Filtering + Anti-Malware, DLP ...

- CASB(Cloud Access Security Broker)
  : 기업이 인가한 SaaS 서비스 통제 및 모니터링에 초점
  : SaaS Visibility, SaaS Control, Authentication, SSO + Anti-Malware, DLP ...



Application Delivery Leader MONITORAPP

❖ CASB Deployment modes

Capabilities for CASB Use Cases and Modes

Type of Cloud Apps	Endpoints	Deployment Mode	Cloud App Discovery and Risk Reporting	Adaptive Access Control	UEBA or DLP (Scan/Remediate)	UEBA or DLP (Real-Time Monitoring)	UEBA or DLP (Enforce on Read)	UEBA or DLP (Enforce on Write)	Threat Protection (Malware Defense)	Precloud Encryption and Tokenization	DRM or Client-Facing Encryption	BYOK Encryption Key Management
Unapproved Cloud	Managed	SWG	3	1		1	1	1				
		CASB Forward Proxy Mode		2		2	2	2	3	2	2	
		CASB Reverse Proxy Mode										
		CASB API Mode										
Approved Cloud	Managed	SWG	3	1		1	1	1				
		CASB Forward Proxy Mode	2	2		2	2	2	3	2	2	
		CASB Reverse Proxy Mode		3		3	3	3	3	3	3	
	Managed & Unmanaged	CASB API Mode			3	3		2	3		3	3

3 Better 2 Good 1 Adequate

Source: Gartner
ID: 393383

- API : CASB와 클라우드 서비스의 직접 통합(클라우드 서비스 제공자의 API 구성에 따름)
- Forward : PAC, Agent, Connector 등을 이용하여 CASB로 트래픽을 유입
- Reverse : 클라우드 서비스 제공자 또는 ID 공급자에서 트래픽을 CASB로 리다이렉션

❖ ZTNA Vs VPN

- ZT : 아무것도 신뢰할 수 없다는 가정하에, 사용자 및 다양한 정보를 바탕으로 최소한의 권한과 세밀한 통제를 지속적으로 수행하는 보안 활동

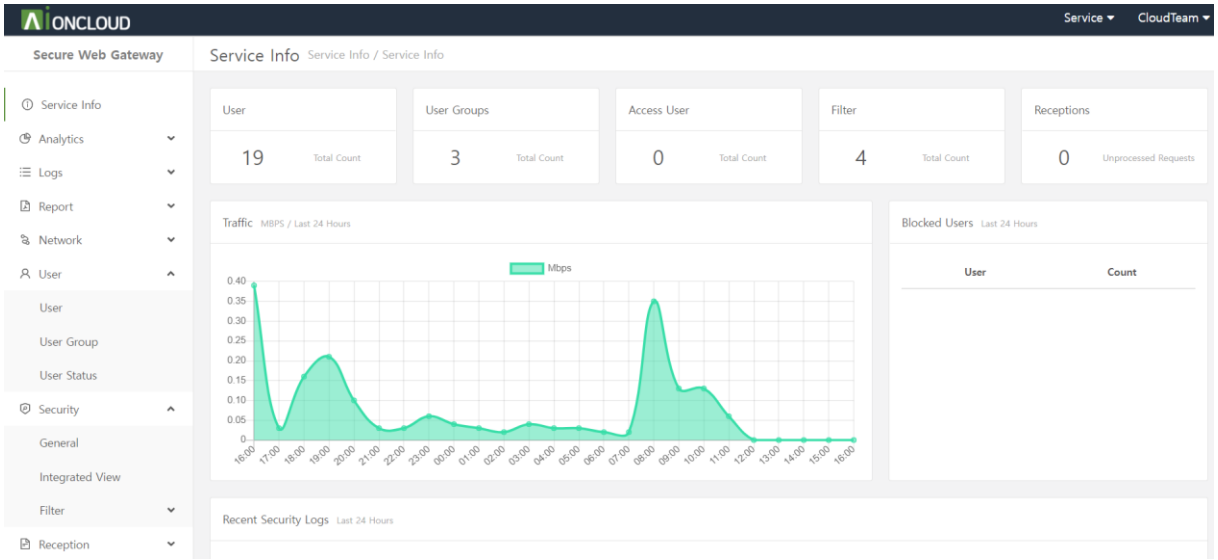
- ZTNA : 애플리케이션별 권한으로 제로 트러스트 보안 원칙을 구현하는 안전한 원격 액세스

	VPN	ZTNA
Layer	Network	**Application**
Perimeter access	Physical	**Logical**
Cloud-based resources	Split tunnel or Backhaul	**Directly**
BYOD endpoint	Accept or reject	**ID and Context**

❖ Pros of SASE/SSE

- 복잡성을 최소화한 간단한 정책 관리
  : 단일 콘솔에서 모든 사용자와 엔드포인트, 그리고 애플리케이션에 대한 엑세스를 관리

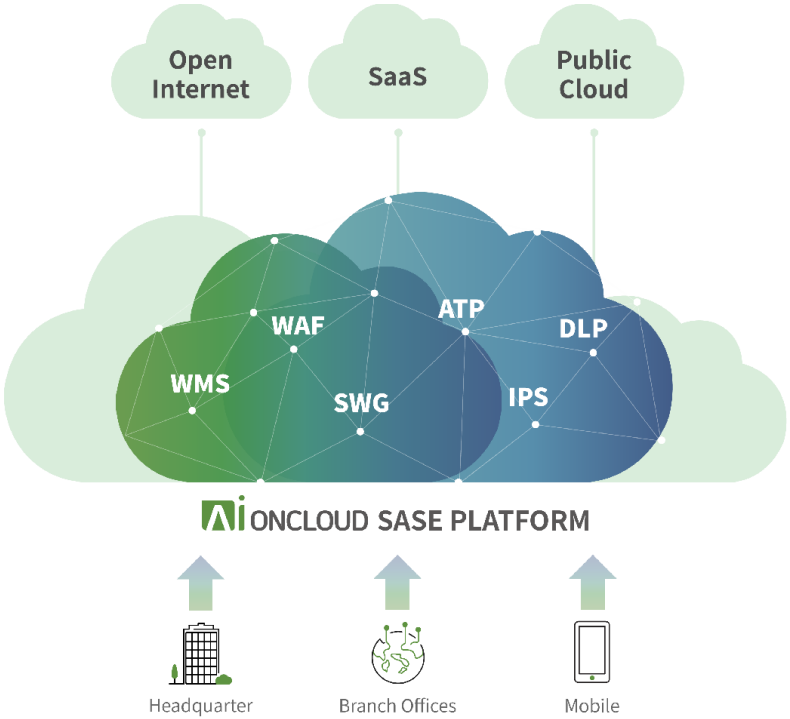
- 플랫폼 자체에서 제공하는 디지털 경험 모니터링
  : 누가 어디를 많이 접속하는지, 악성 사이트에 접속한 사용자는 누군지
  민감한 파일에 접근한 사용자는 누구인지 등...



02. Global Edge 플랫폼 AIONCLOUD

❖ AIONCLOUD(Application Insight on Cloud)

AIONCLOUD는 기존 네트워크 보안 기술에 대한 현대적인 대안입니다.
복잡한 네트워크 분할을 요구하지 않고 클라우드 서비스를 통해 최종 사용자에게 보안 연결을 확장하여,
사용자는 언제 어디서든 기업 네트워크에 연결 하거나 인터넷에 안전하게 액세스 할 수 있습니다.



Application Delivery Leader MONITORAPP

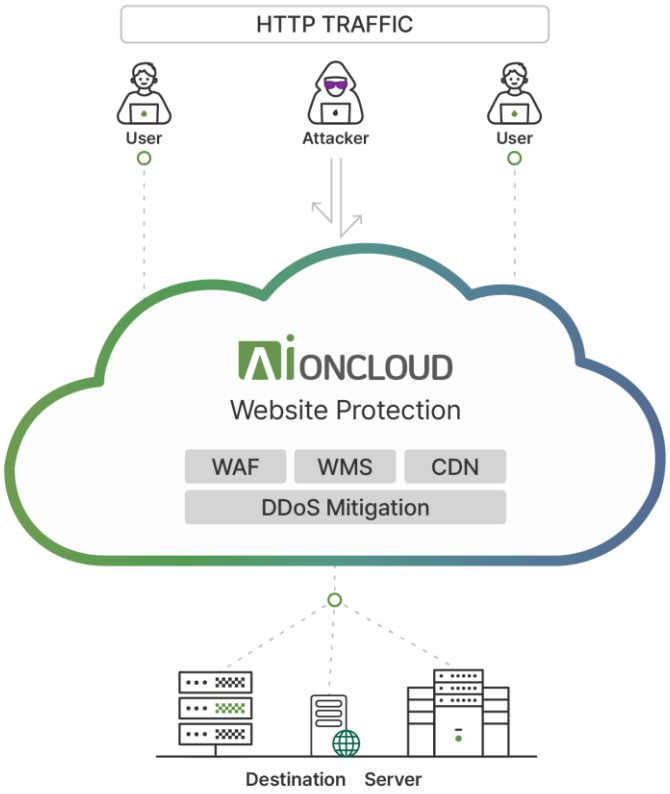
❖ AIONCLOUD Global network

- 전체 네트워크 보안 스택을 클라우드 기반 서비스 플랫폼으로 제공
- 모든 사용자, 모든 엔드포인트, 모든 애플리케이션에 대한 엑세스를 관리할 수 있는 싱글 포인트
- 전통적인 기존 경계선 보안 아키텍쳐의 한계점을 극복하고 **제로 트러스트 원칙 실현**
- 15개국 40개 IDC에 배치된 AISASE 플랫폼 간 상호 연계를 통한 멀티테넌시 서비스 인프라

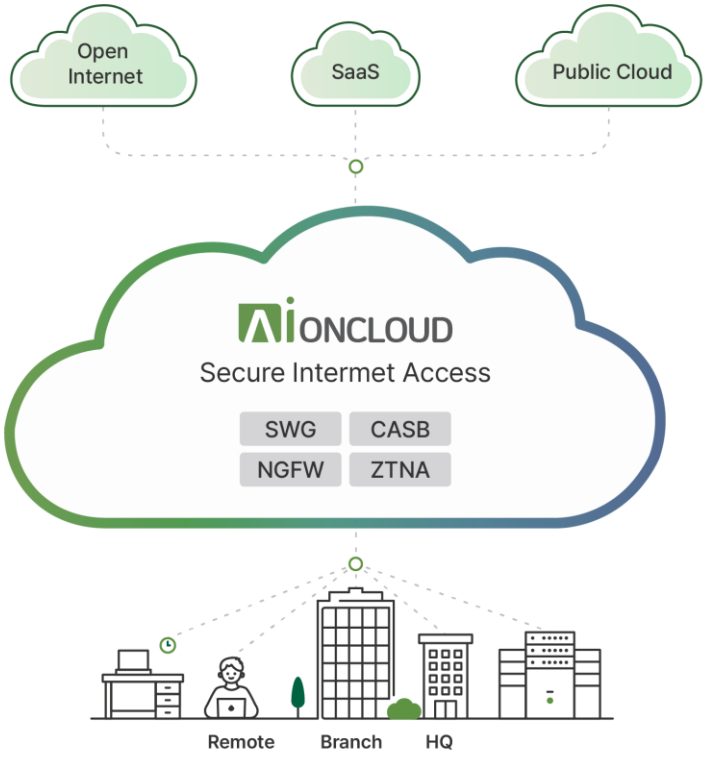
❖ AIONCLOUD Service Category

- **Website Protection : 기업 데이터센터에 대한 보안 서비스**
- **Secure Internet Access : 내부 사용자의 안전한 인터넷 연결을 보장하는 보안 서비스**

Website Protection



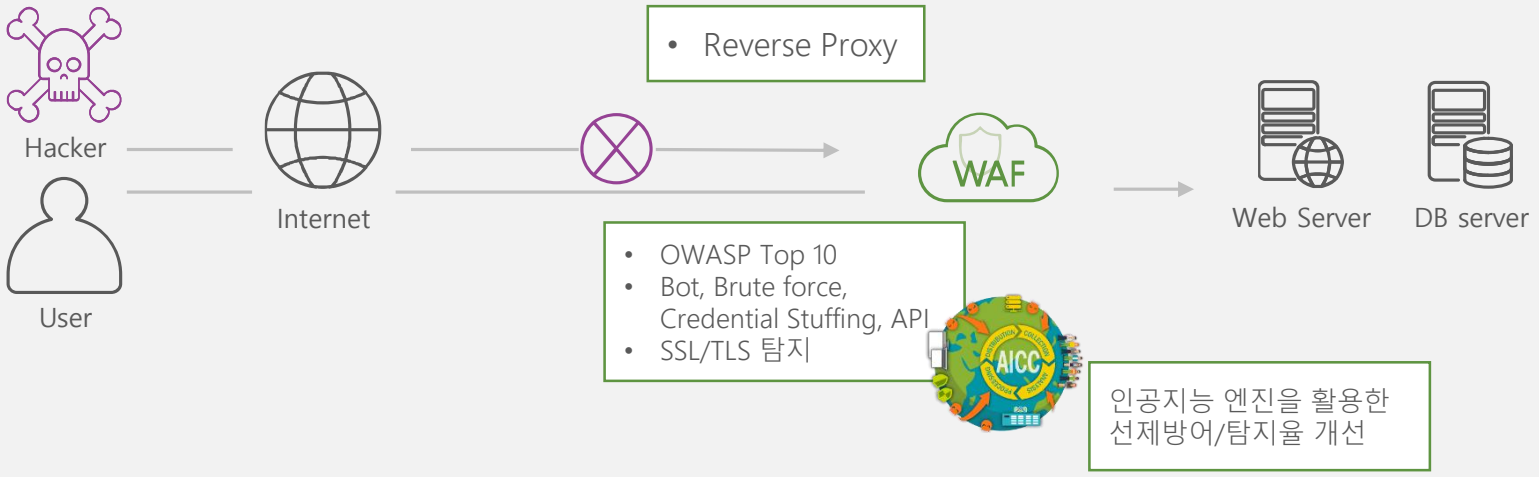
Secure Internet Access



❖ Website Protection

- 기업 내부/데이터센터로 유입되는 보안 위협으로부터 방어
- CDN(Content Delivery Network) / WAAP(Web Application & API Protection) / WMS(Website Malware Scanner) 서비스로 구성
- HW / SW 설치, 유지보수, 라이센스가 필요 없는 강력한 웹 보안과 성능 최적화를 제공

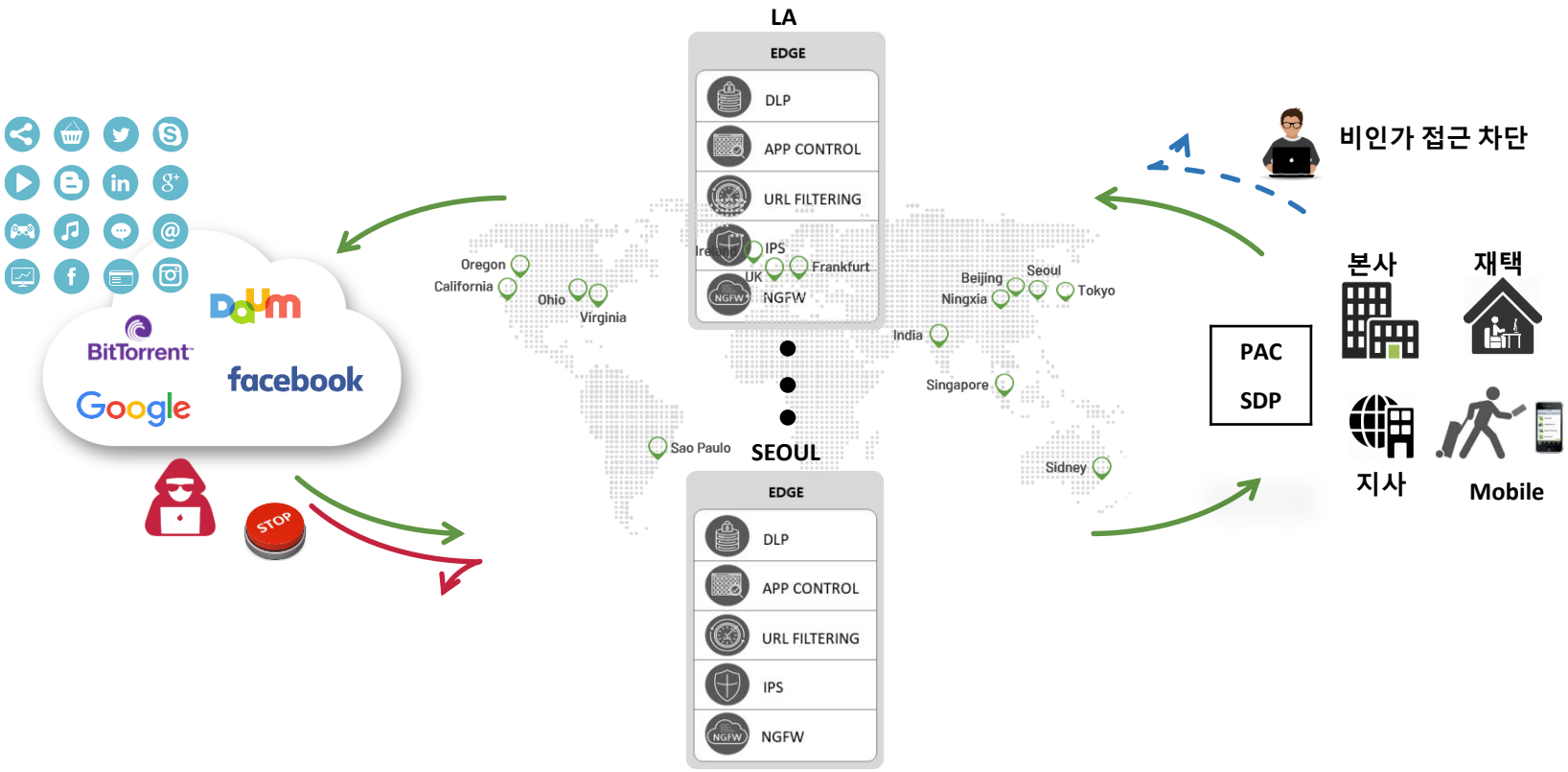
WAAP 서비스 구성



Application Delivery Leader MONITORAPP

❖ Secure Internet Access

- 사용자가 외부 인터넷 이용 시 발생할 수 있는 보안 위협 제거
- SWG(Secure Web Gateway) / CASB(Cloud Access Security Broker) 서비스로 구성
- PAC / AISASE Connector를 통해 언제 어디서든 일관된 보안 서비스 이용



Application Delivery Leader
MONITORAPP

THANK YOU

MONITORAPP

㈜모니터랩 | 주소 : 서울시 구로구 디지털로 27가길 27 아남빌딩 8,9층 08375 | Tel : 02-749-0799 | Fax : 02-749-0798 | Web : www.monitorapp.com
E-mail : sales@monitorapp.com | 사업자등록번호 : 214-87-66413 |