Hewlett Packard Enterprise

SD-WAN과 클라우드 보안 서비스의 만남, SASE (EdgeConnect SD-WAN & SSE)

이한민 매니저

Nov, 2023

SD-WAN / SASE Overview

기존 네트워크 접근 방식의 한계

중앙 또는 관문 방화벽으로의 단순한 인터넷 트래픽 전송은 장비의 성능을 낮추고, 대역폭을 낭비하며, 정책 적용이 획일적일 수 밖에 없음

네트워크 전반에 걸친 일관성 없는 보안 정책은 복잡하기만 할 뿐, 위협으로부터 정보 자산을 보호하기 어려움

기존의 VPN은 원격지에서의 내부 접속 경로만 제공할 뿐, 사용자 기반의 수준 높은 보안 정책이나 클라우드 환경에 대응하지 못함

일하는 방식이 변화함에 따라 데이터가 저장되는 위치도 변화

하이브리드 및 원격 근무가 연결성을 제공하는
새로운 솔루션의 필요성을 혁신적으로 이끌어냄

언제 어디서나 쉽게 접근할 수 있는
애플리케이션과 **개인 정보**에는
새로운 **보안 정책과 접근 제어**가 필요함

SASE란?

Secure Access Service Edge = SD-WAN + SSE(Security Service Edge)

Secure SD-WAN

- Advanced, Secure SD-WAN
- Dynamic Routing
- WAN Optimization
- Next Generation Firewall
- IDS/IPS
- DDoS Protection
- Advanced Segmentation

ICSA labs CERTIFIED SECURE SD-WAN

EdgeConnect SD-WAN
EdgeConnect SD-Branch
EdgeConnect Microbranch

Security Service Edge (SSE)

- Zero Trust Network Access
- Cloud Access Security Broker
- Secure Web Gateway
- Firewall as a Service
- Remote Browser Isolation
- Data Loss Prevention
- Sandboxing

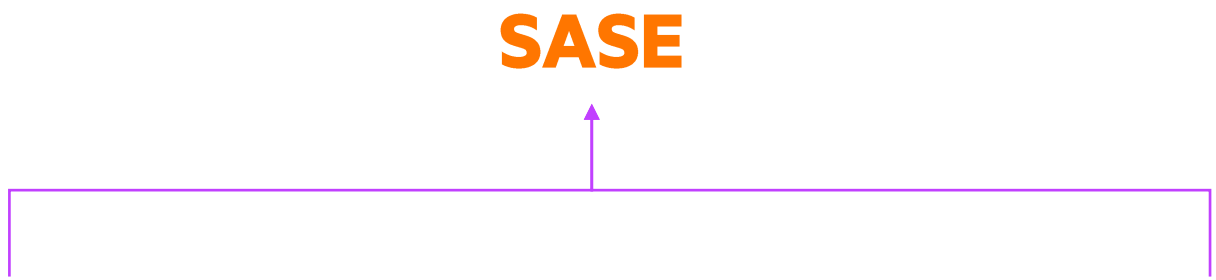
Automated integration with cloud security partners

zscaler, netskope, PRISMA, CHECK POINT, McAfee, iboss, Symantec, Lookout, FORCEPOINT, axis

Choice & flexibility with no compromise to networking or security

유연한 SASE 구성

Single or Dual vendor



Single-vendor SASE

네트워크와 보안을 하나로 통합

구성과 설정의 복잡도 최소화

axis

Dual-vendor SASE

자유롭고 유연한 솔루션 선정

원활한 통합으로 작업 난이도를 줄임

zscaler netskope

EdgeConnect SD-WAN 개요

SD-WAN의 주요 기능

경로 최적화, WAN 가속 기능, 실시간 애플리케이션 트래픽 및 회선 품질 모니터링

Path Conditioning

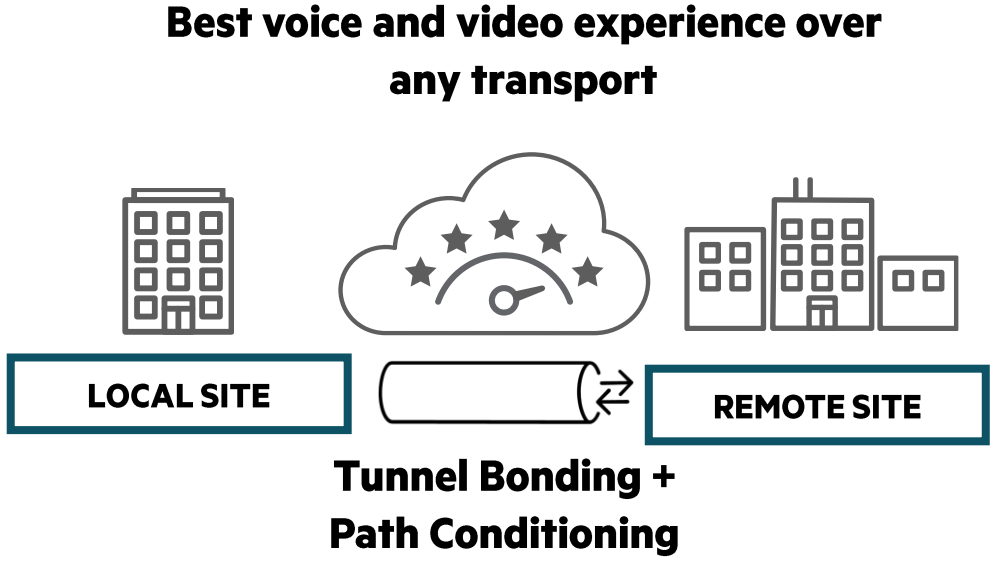
- Overcome the adverse effects of dropped and out-of-order packets that are common with broadband internet and MPLS connections

WAN Optimization

- Leverage TCP Protocol acceleration and data compression techniques
- Find the best path and the shortest route to the closest point of presence to accelerate SaaS applications

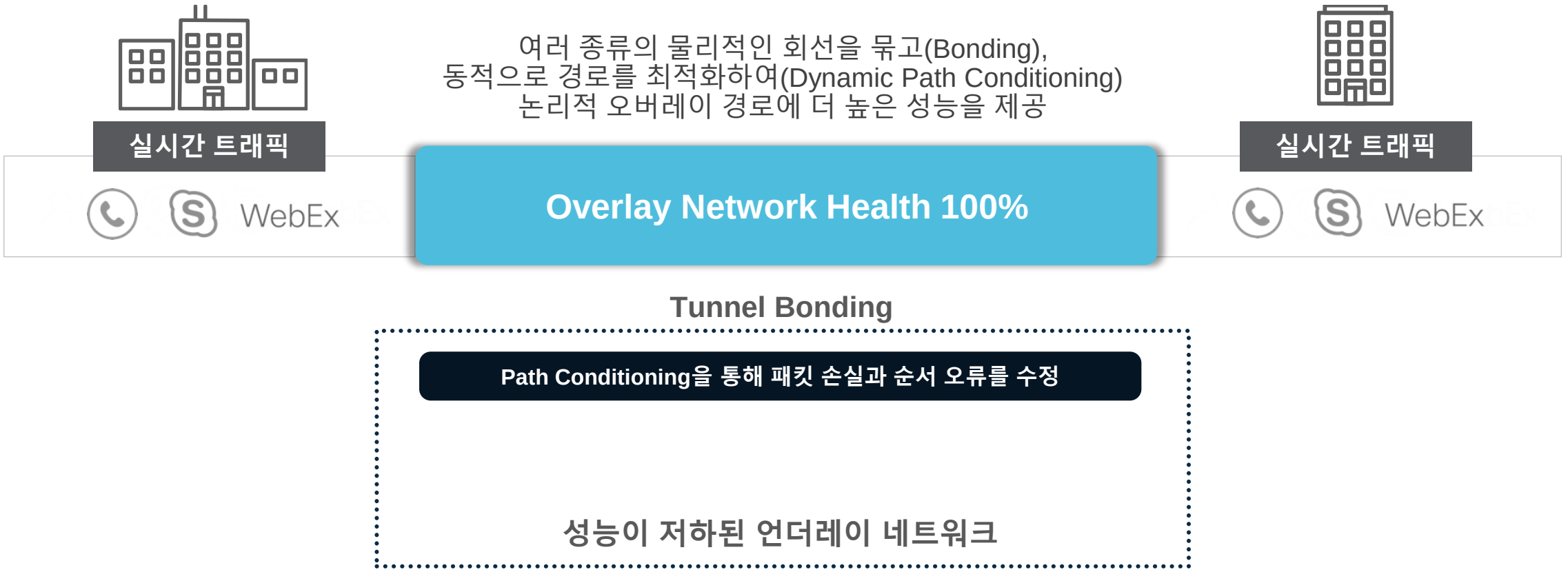
Real time Applications

- Experience consistent application performance including high quality voice and video over broadband connections.



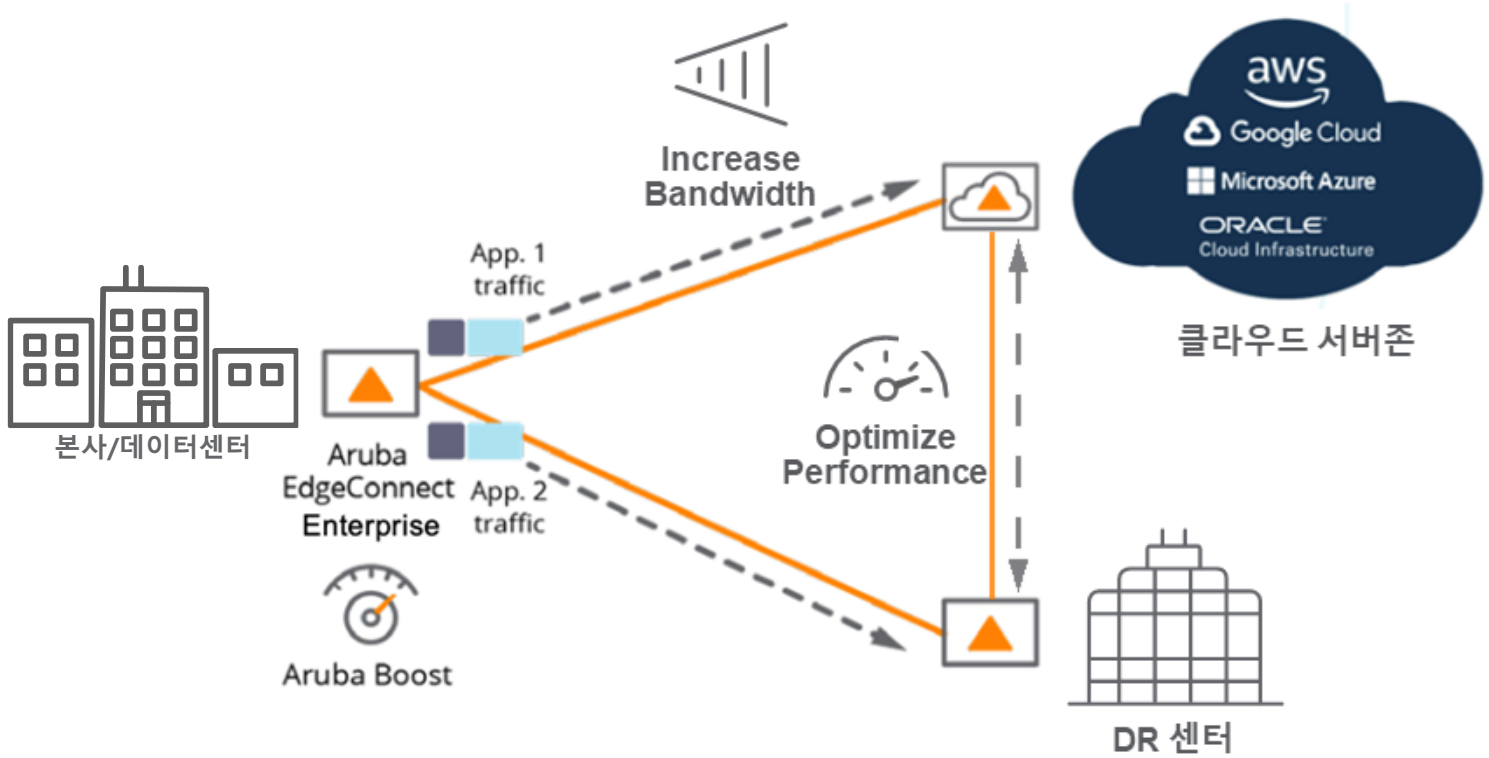
고품질의 회선 서비스를 안정적으로 제공

언더레이 회선의 결합을 통한 최적 품질의 SD-WAN 오버레이 제공



WAN Optimization

TCP 가속 및 데이터 최적화를 통한 애플리케이션 성능 향상 및 회선 효율화



애플리케이션 성능 향상

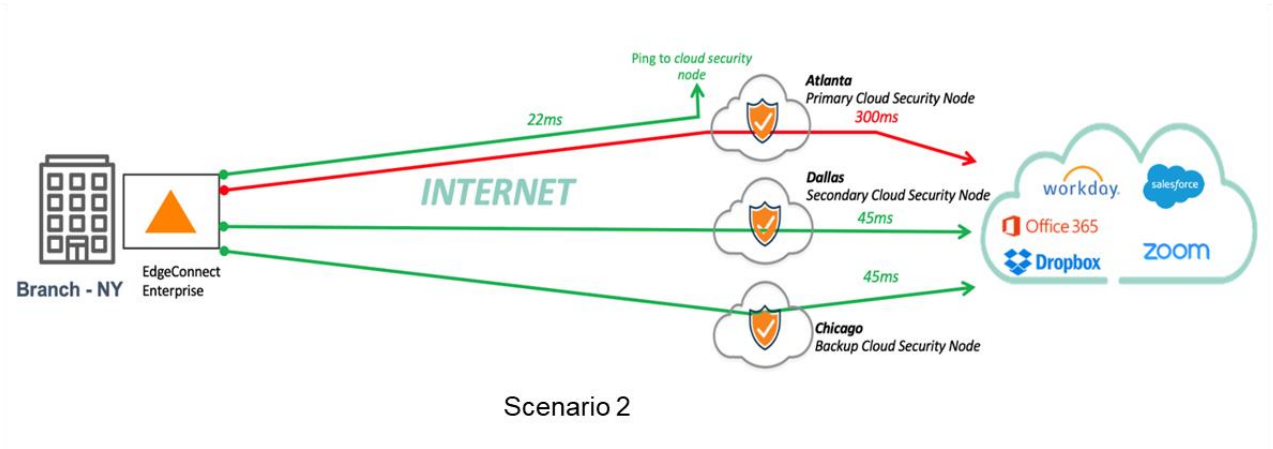
데이터 압축 / 중복제거 회선 사용 효율화

데이터 백업 / DR

회선 / 클라우드 비용 절감

App Express

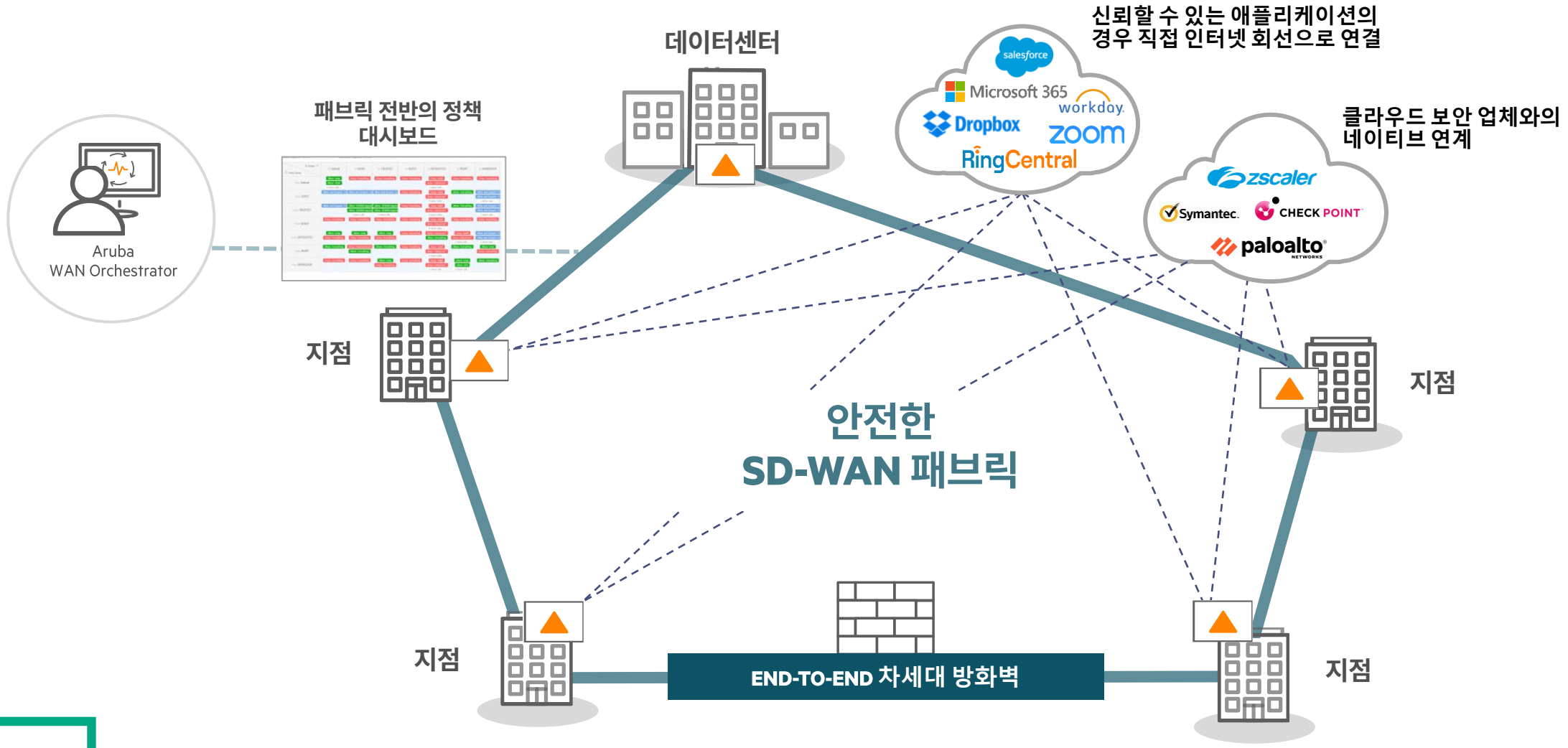
상시적으로 SaaS 접속 경로 데이터를 업데이트하며, 최적 경로를 제공



- 복합 측정 지표를 통해 애플리케이션별 실제 트래픽의 응답 속도를 주기적으로 측정하여 최적 경로를 선택
- 시나리오 1 환경에서는 두 ISP 회선 중에서 응답 속도가 빠른 ISP2 경로가 선택됨
- 시나리오 2 환경에서는 Primary Cloud Security Node까지의 응답 속도는 Atlanta 구간이 빠르지만 애플리케이션 최종 응답 속도가 낮으므로, Secondary Node인 Dallas 경로가 선택됨

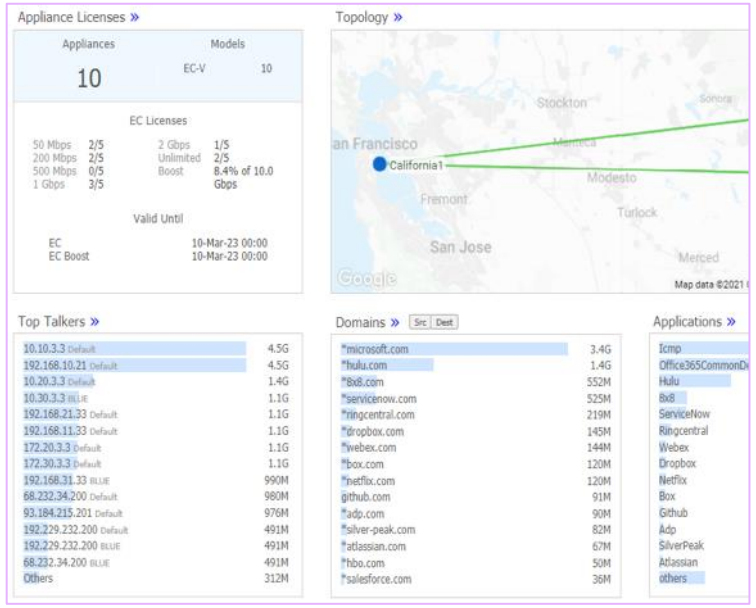
네트워크 격리 및 보안성

세그먼트 기반의 차세대 방화벽을 통해 트래픽을 분리하고 보안성을 제고



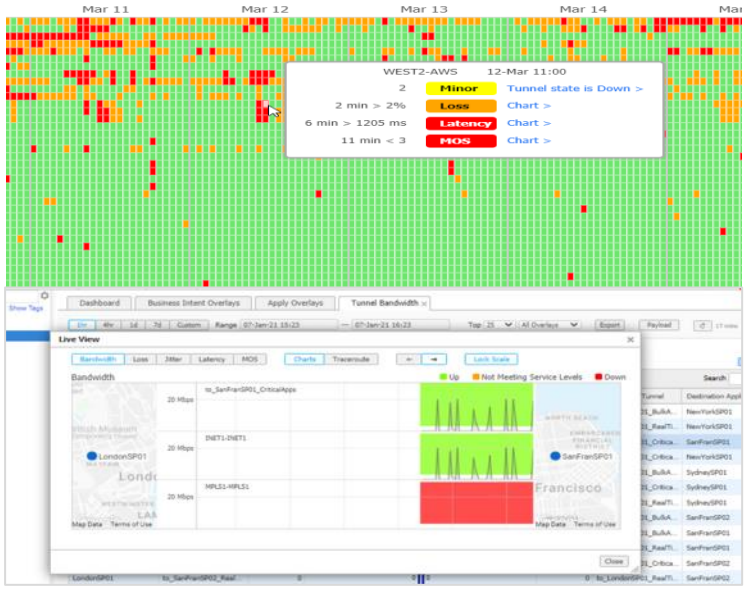
애플리케이션과 네트워크 가시성

대시 보드



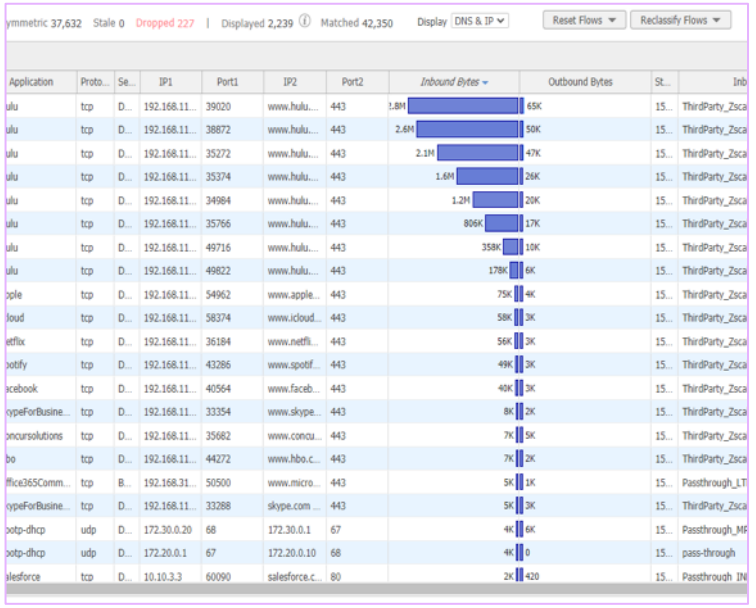
Comprehensive dashboard highlights key network and application attributes, and places focus on critical issues

실시간 장비 상태



Network health is visualized in real-time and correlated across all locations. Alarms, network health and configuration issues are all easily diagnosed

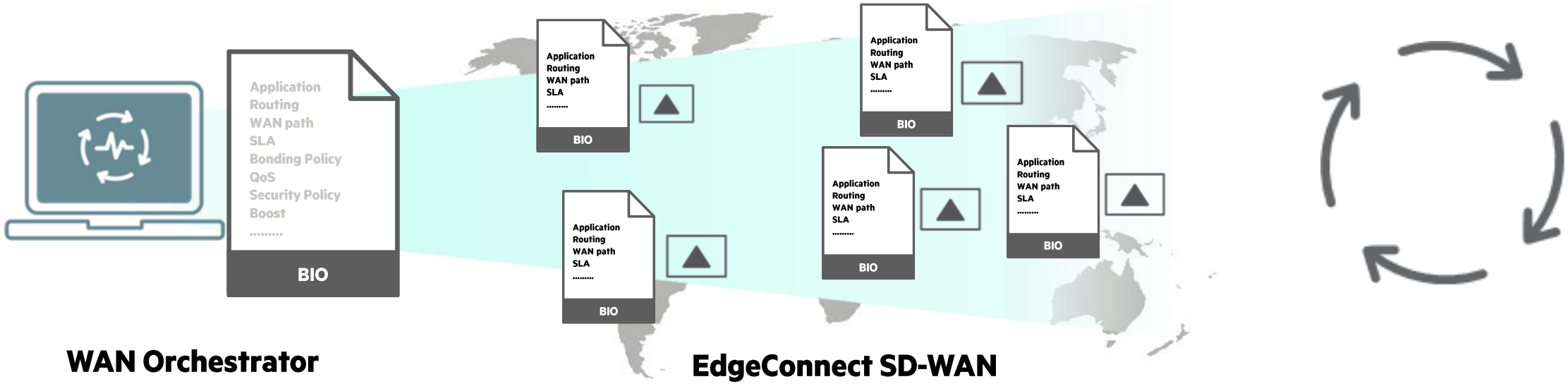
플로우 수준의 트래픽 현황



Flow level statistics give total visibility into every connection on the network providing total visibility and control of applications and users

완전한 자동화

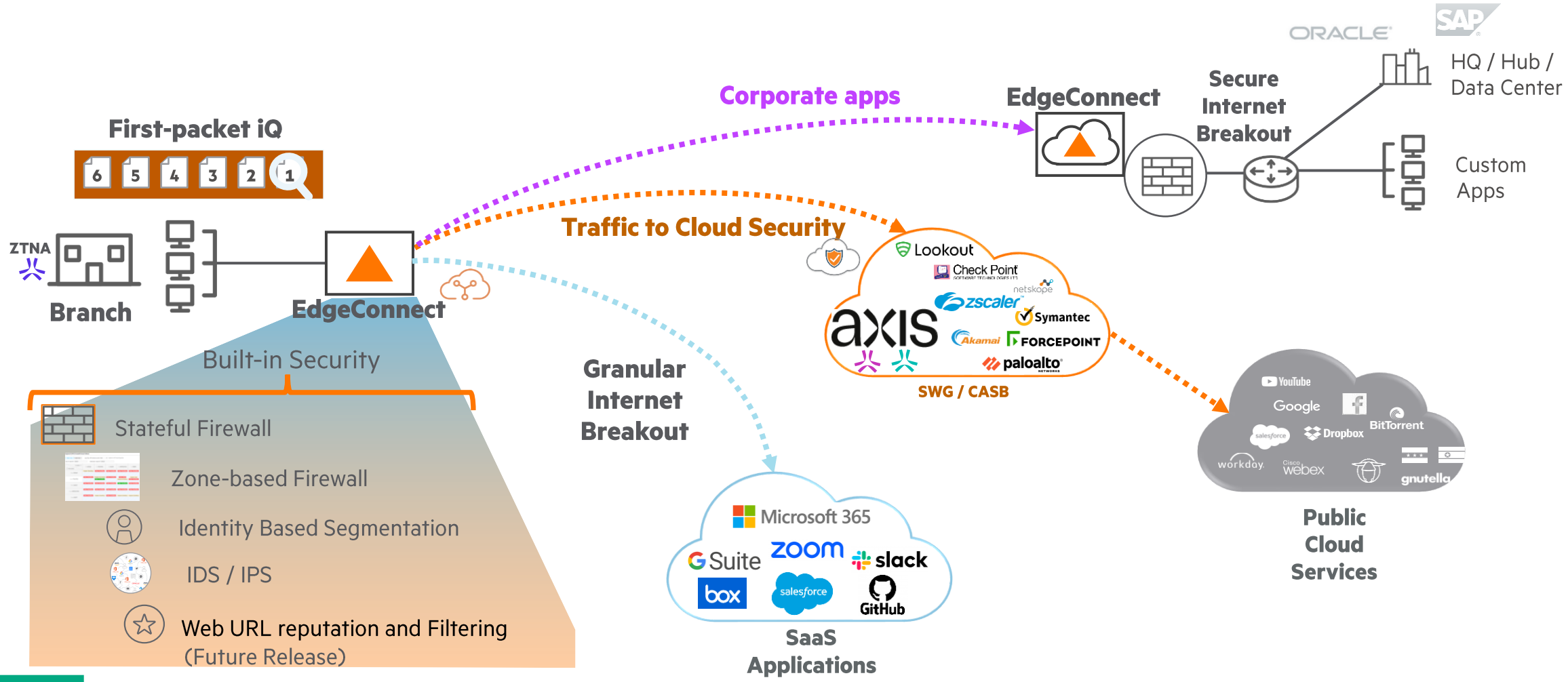
템플릿과 프로파일을 통한 운영 편의성 및 효율화



1. Create Business Intent Overlay (BIO)
2. Push and Maintain Policies Globally
3. Continuously Monitored and Updated

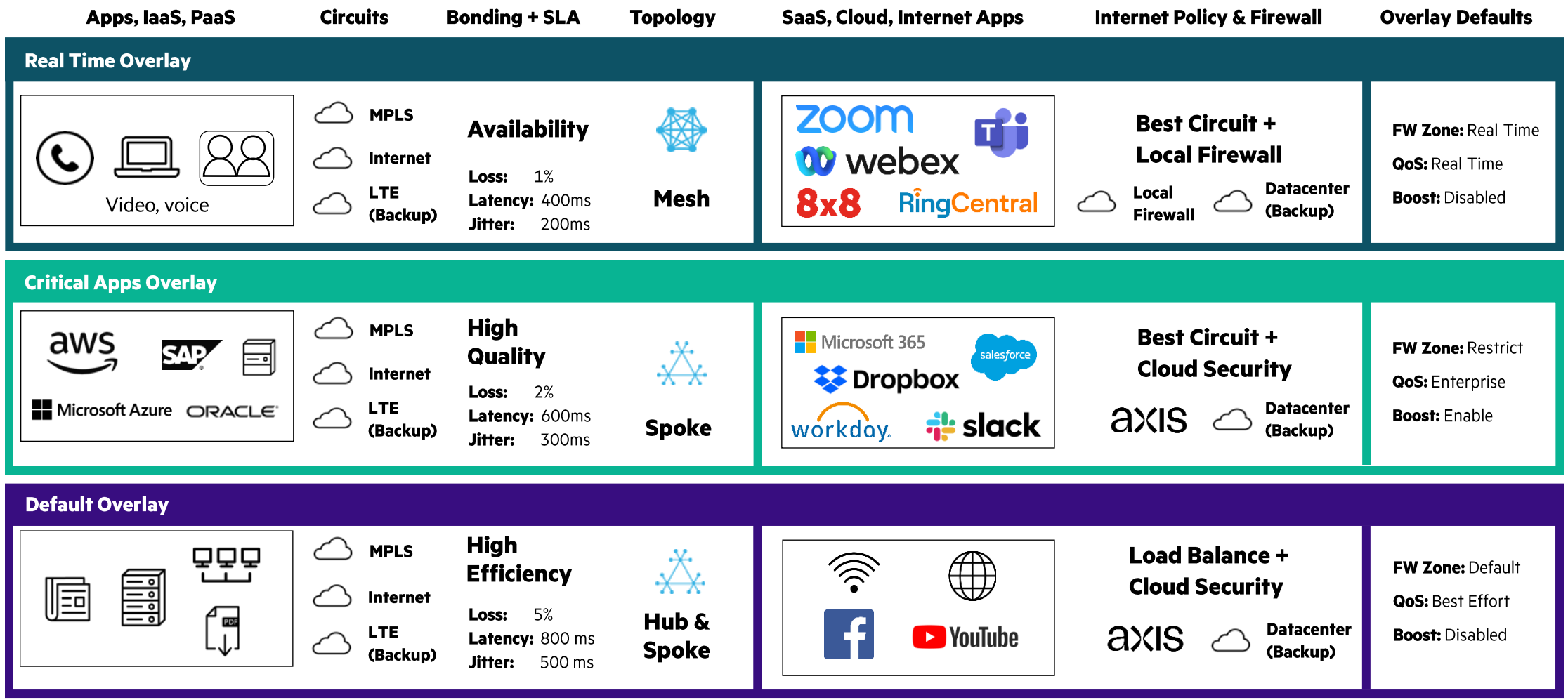
SASE 구성

SSE 솔루션과 결합하여 사용자 및 애플리케이션 접근 보안 적용



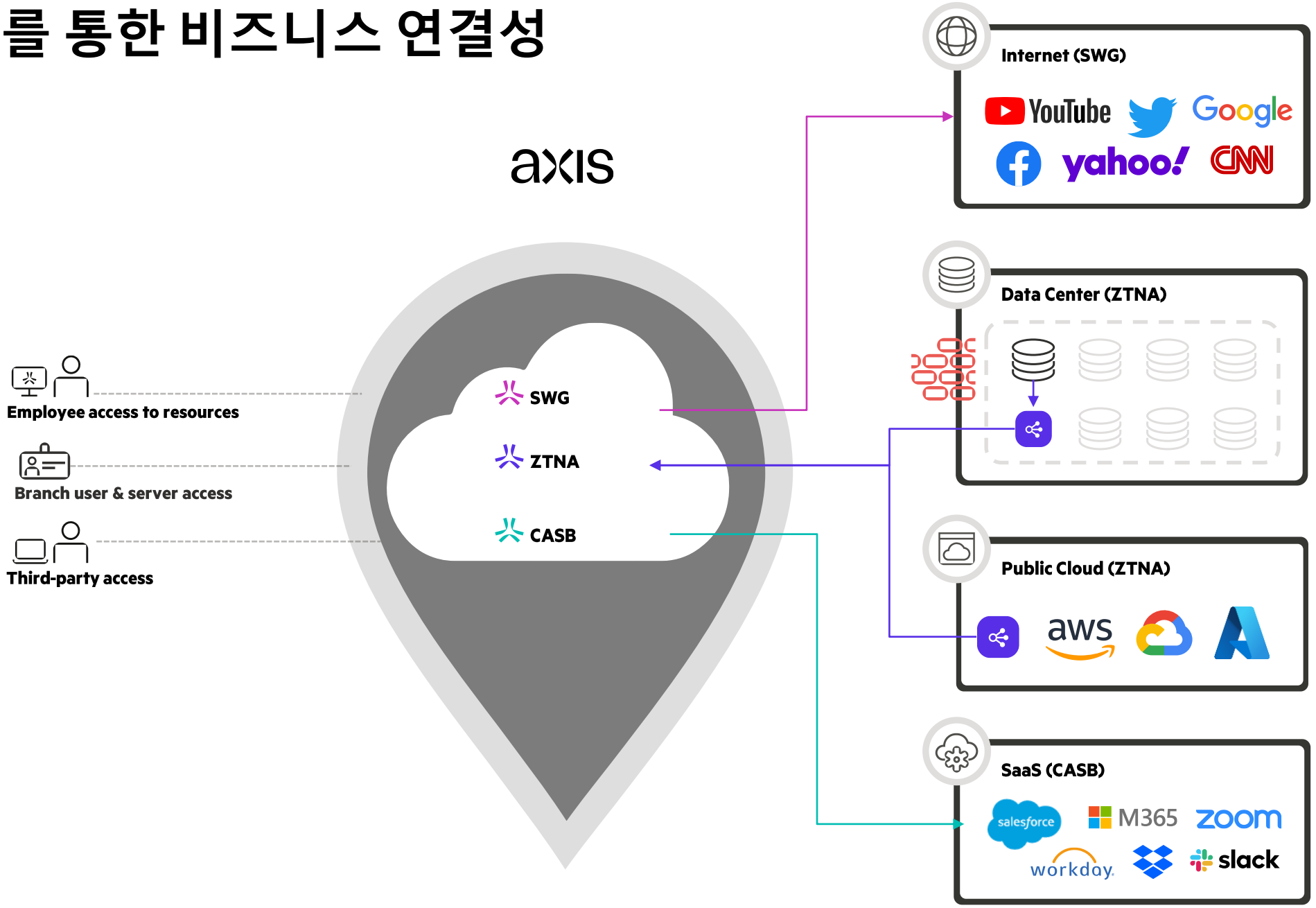
Business Intent Overlay(업무 중심적 네트워크 정책)

GUI 환경에서 손쉽게 SD-WAN 오버레이 정책을 적용



SSE(Security Service Edge) 개요

클라우드를 통한 비즈니스 연결성



SSE 주요 기능

Zero Trust Network Access (ZTNA)

Client or clientless endpoint access solution to securely provision access to network resources.

- Agent / Agentless 기반으로 사용자 Device의 네트워크 접근 제어 및 사용자별 보안 정책을 적용
- Legacy Client VPN의 한계를 넘은 ZTNA 기능 제공

Secure Web Gateway (SWG)

Cloud based firewall to securely access, monitor and inspect all web traffic.

- URL / 컨텐츠 필터링 등의 기술 통해 유해 사이트 및 웹 기반의 사이버 위협으로부터 사용자 Device와 내부 네트워크를 보호

Cloud Access Security Broker (CASB)

Cloud based security to manage, control and monitor user access to SaaS applications.

- 클라우드 환경의 기업 업무 인프라와 SaaS에 대한 사용자 보안 정책 적용
- 클라우드 접근 정책, 가시성, DLP 기능 제공

Digital Experience Monitoring (DEM)

Cloud based security to manage, control and monitor user access to SaaS applications.

- 사용자의 애플리케이션 접근 현황, 사용자 Device의 성능 및 사용자의 접근성에 이슈가 발생했을 때 이를 해결하기 위한 가시성을 제공하는 모니터링 시스템

Agent vs Agentless

기능	Agent	Agentless
모든 포트와 프로토콜 지원 (Any ports and protocols, UDP/TCP)	Y	N
인증서 기반 장치 상태 확인 (Certificate-based device posture checking)	Y	Y
목적지 네트워크 범위 지정 (Destination Network Ranges)	Y	N
호스트 기반 클라이언트 애플리케이션 (Host-based client applications)	Y	N
서버 또는 VoIP 장치와 같이 장비 기동과 동시에 IP 주소가 지정되어야 하는 애플리케이션 지원 (Applications that require the specific IP address of the devices, such as server-initiated or peer-to-peer such as VOIP)	Y	N
SaaS 애플리케이션	Y	N
파일 공유 (SMB)	Y	N
전반적인 장치 상태 확인 및 제한적인 보안 정책 적용 (Requires comprehensive device posture checks and more restrictive security policy)	Y	N
SSH 애플리케이션 범위 지정	Y	N
Agent less 방식의 Web, RDP, SSH, Git, MS SQL Database 제어 (Web, RDP, SSH, Git, and MS SQL database with seamless user experience and granular visibility/control without installing anything in the device)	N	Y

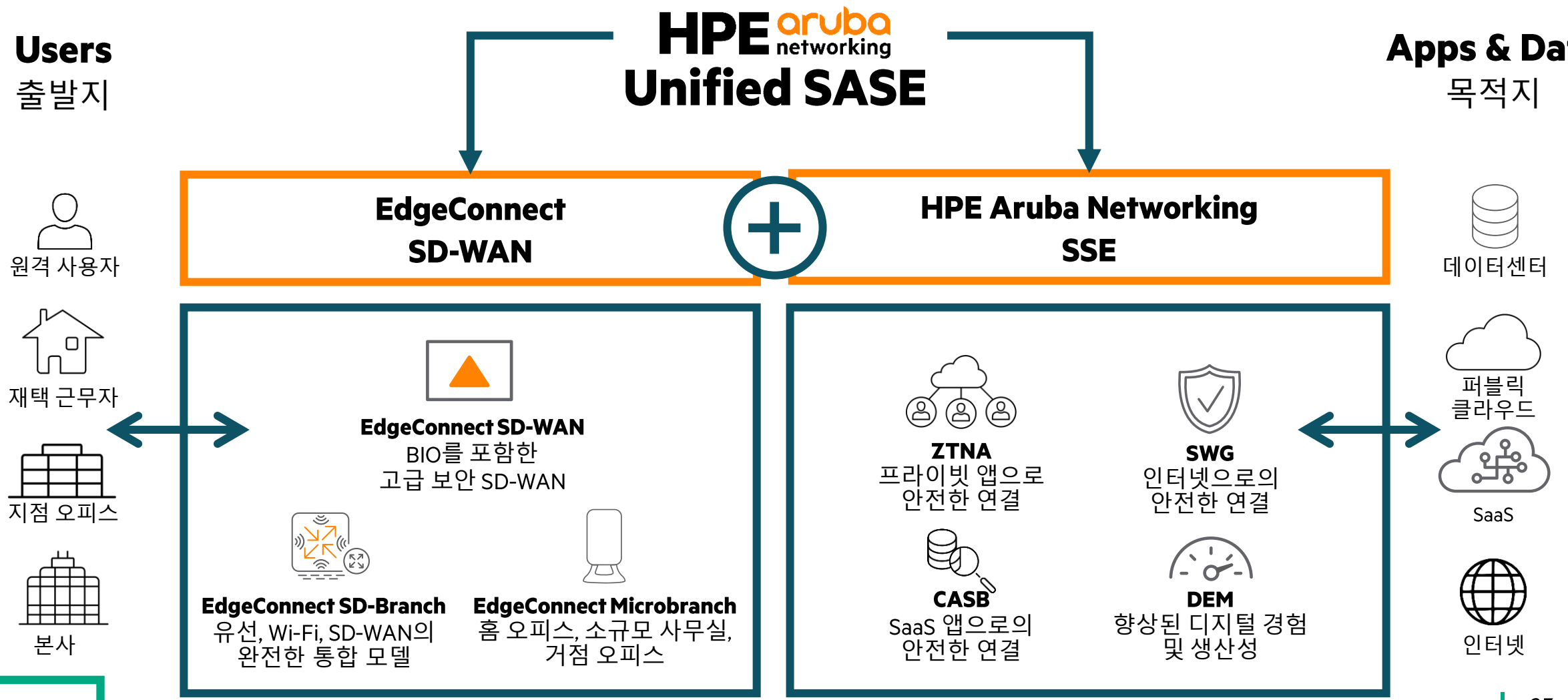
SSE 이용 사례

1. IP/VLAN 기반 Client VPN 정책(ACL)이 아닌 SaaS 및 애플리케이션 정책을 적용
2. Agent 설치 없이 웹 브라우저 인증서 기반으로 RDP, SSH, 웹 접속 및 모니터링 기능 제공
3. 하드웨어 장비 구축 없이 클라우드 기반의 SWG 도입
4. Google Workspace, Okta 등 다양한 IdP를 이용한 SAML 연계 사용자 관리
5. 방화벽과 바이러스 백신이 활성화된 디바이스에서만 내부 시스템 접근을 허용
6. 클라우드 단일 관리 화면에서 모든 정책 적용과 모니터링 및 트러블슈팅 진행

Summary

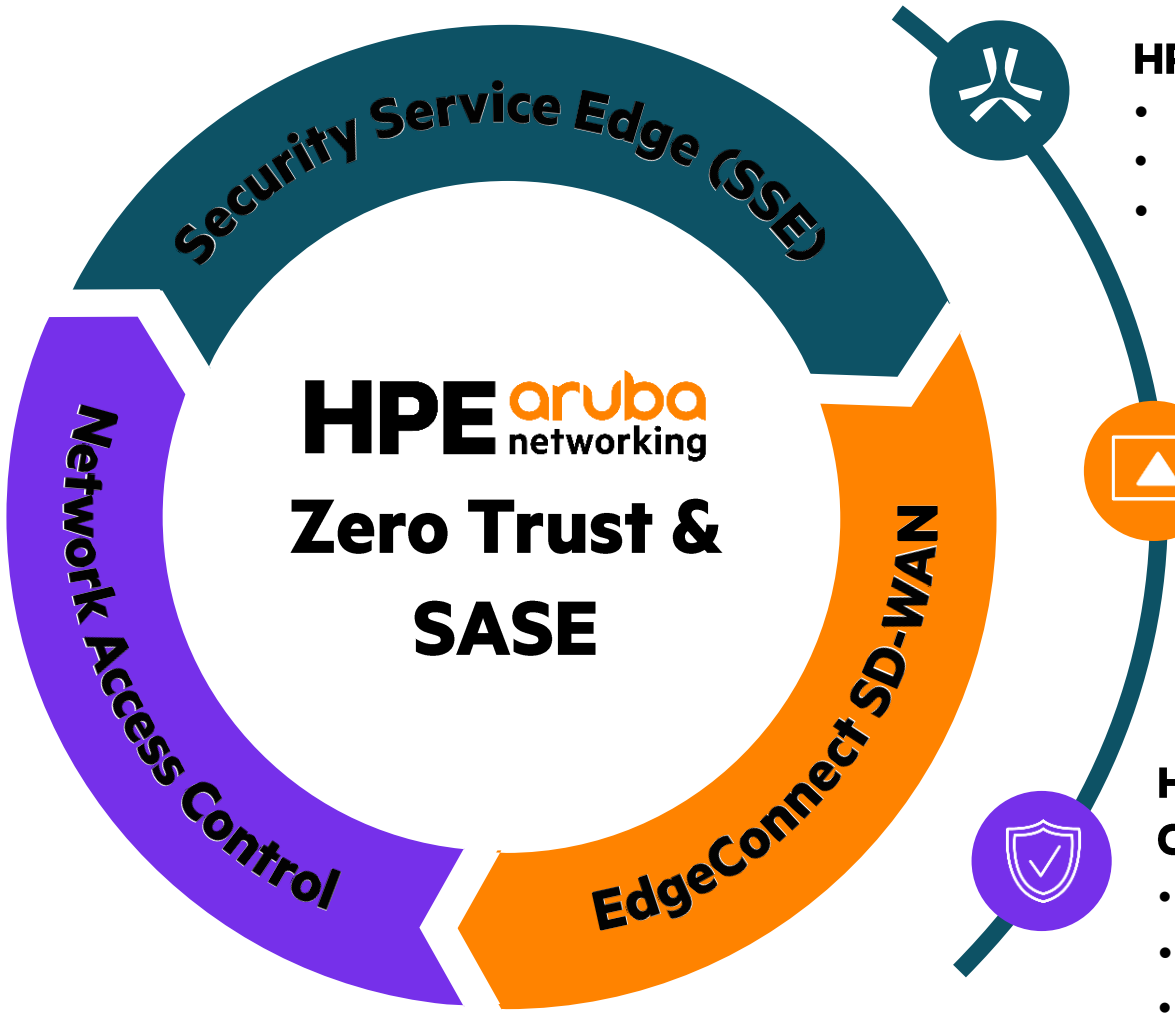
HPE Aruba Networking Unified SASE

업계를 선도하는 SD-WAN 솔루션과 클라우드 네이티브 SSE 솔루션의 결합



HPE Aruba Networking의 Zero Trust 및 SASE 전략과 방향성

제로 트러스트 보안을 적용하여 연결 위치에 관계없이 사용자와 애플리케이션을 보호



HPE Aruba Networking SSE

- Agent/Agentless ZTNA
- 통합 정책 관리
- Global PoP(Point of Presences):
  - 시드니, 홍콩, 싱가포르, 뭄바이 (in APJ Region)

EdgeConnect SD-WAN

- 보안 SD-WAN
- 멀티 클라우드 지원
- QoE 향상

HPE Aruba Networking Central NetConductor & ClearPass NAC

- 인공지능 기반의 클라이언트 시각화 및 프로파일링
- Dynamic Segmentation
- 지속적인 모니터링

SASE 솔루션 영상

클릭! →

Thank you

이한민 매니저
jake.yi@hpe.com