제로 트러스트 익스체인지

베스핀글로벌

문의 / zerotrust@bespinglobal.com

BESPIN GLOBAL
HELPING YOU ADOPT CLOUD.

Agenda

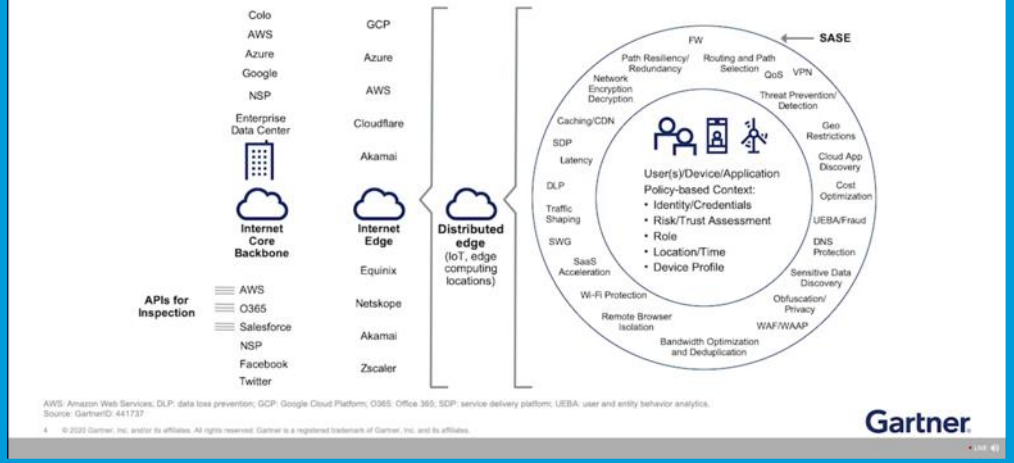
1. Secure Service Edge & SASE NEW
2. Zero Trust Exchange 마켓 평가 NEW
3. 변화의 방향
4. Zscaler 솔루션
5. 기술 파트너 ECO
6. Zscaler 도입 효과
7. 보안 정책, 서비스 운영의 방향
8. CASE

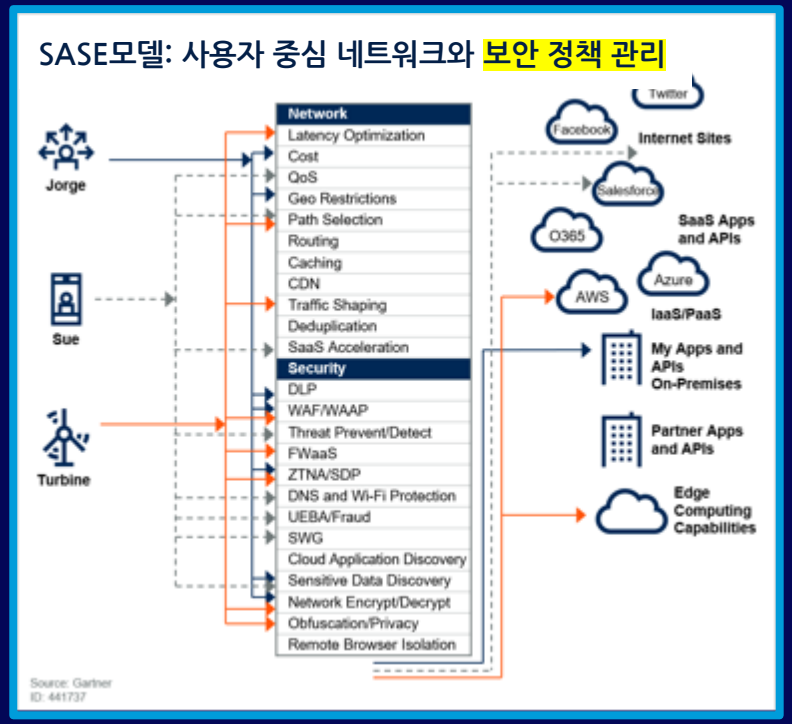
Secure Service Edge & SASE

인터넷 + 보안의 정의, SASE 아키텍처 (가트너 자료 참조)

- 네트워크 중심 -> 사용자 중심
- 네트워크 보안 -> 사용자 보안
- 보안기능 중심 -> 보안 정책 규정 준수
- 보안장비 관리 -> 서비스 및 정책 통합 관리

사용자 중심 보안 서비스





SASE에서 SSE (Secure Service Edge)의 정의

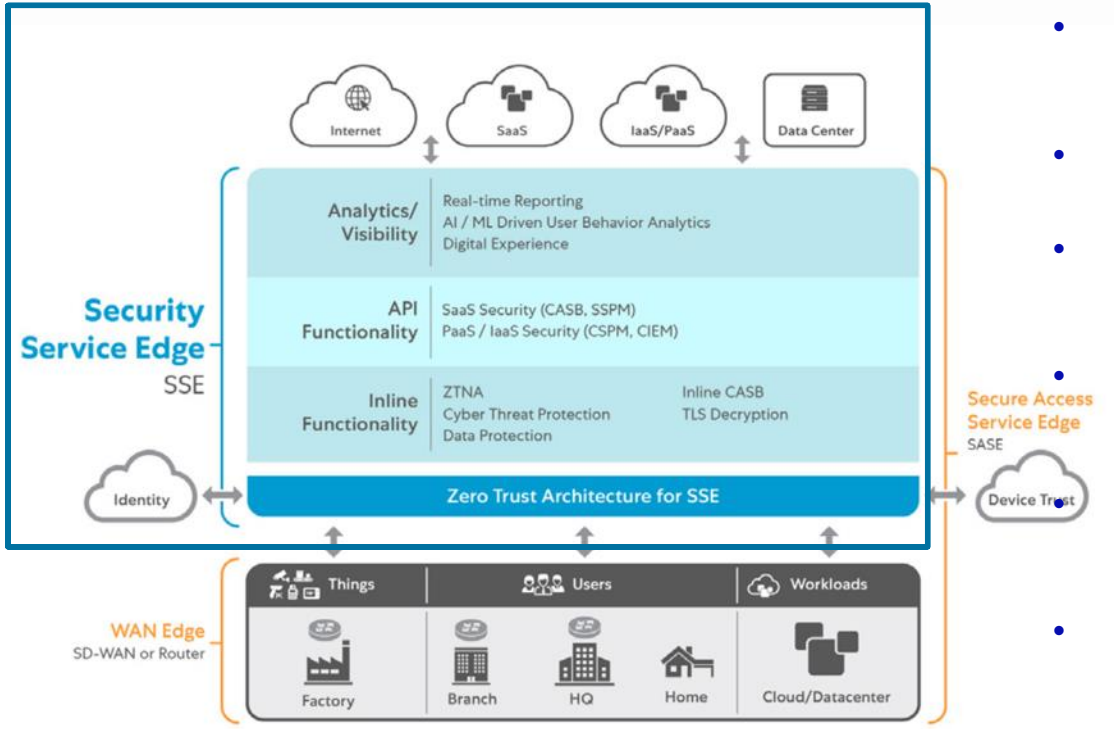


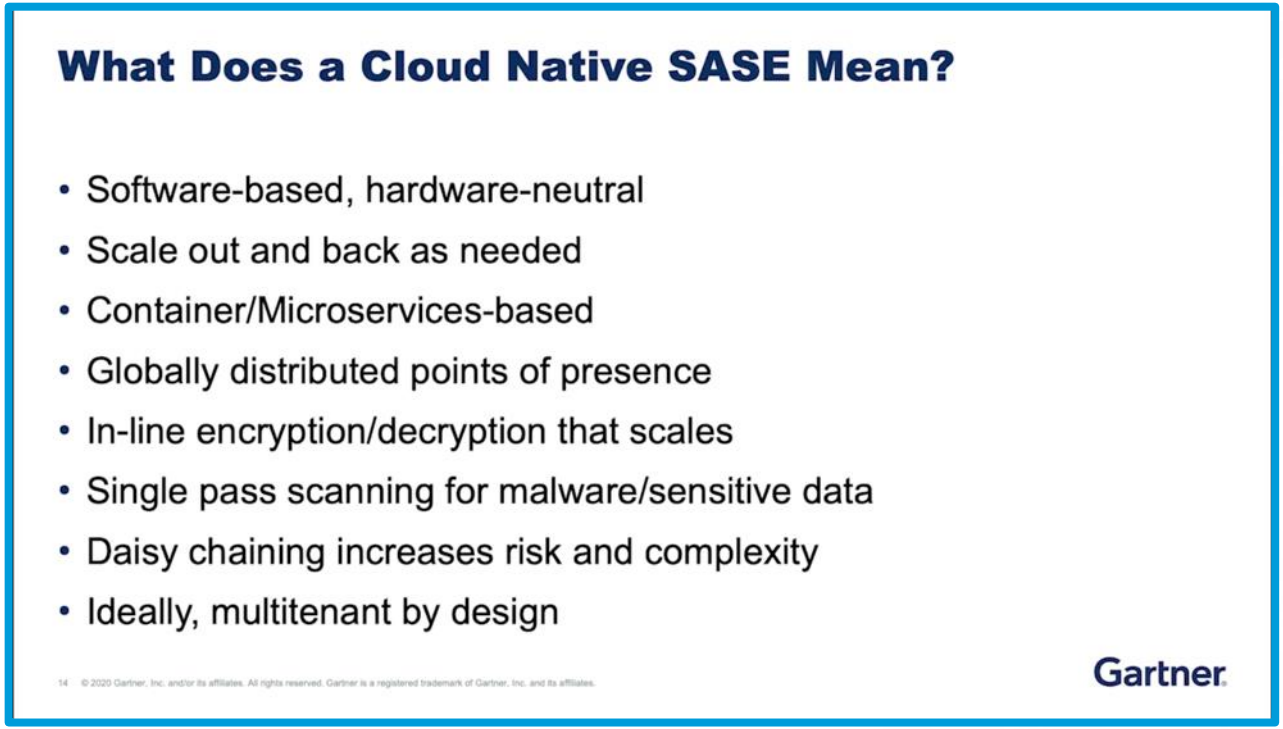
Figure 1: The Secure Access Service Edge (SASE) framework includes SSE for policy decision and enforcement. SASE requires the use of dedicated connectivity solutions from the requesting entity and the security edge where policy is enforced.

- SSE(Security Service Edge)는 SASE(Secure Access Service Edge) 프레임워크의 구성 요소로서 WAN 구간을 제외한 보안 정책 결정 및 시행에 대한 정의입니다.
- SSE는 통합 보안과 클라우드 플랫폼으로 제공 “보안 및 연결”을 의미합니다.
- 아키텍처 단순성은 항상 기업에게 이점이 됩니다. 특히 이러한 단순성으로 기술적 문제가 최소화되고 비즈니스가 가속화될 수 있습니다.
- 많은 조직에서 보안은 불편함, 병목 현상을 일으키는 장애물, 민첩성을 제한하는 게이트키퍼 또는 비즈니스 가속의 장애물로 간주되고 있었습니다.

SSE는 이러한 고정관념에 넘어서고, SSE 환경에서 보안은 보호 및 제어 (Protection & Control)을 제공하며 비즈니스 민첩성을 제공 합니다.

- 2019년에 도입된 SASE 프레임워크는 클라우드와 모빌리티, 디지털화를 주요 목표로 합니다. SASE는 네트워크 액세스와 보안을 통합하며 클라우드 에지(SSE)로부터 서비스를 제공합니다(그림 1 참조).
- SSE는 보안이 중앙 집중화 되지 않도록 하고, 어디에서나 모든 사용자의 안전한 연결 (Secure Connection)을 제공 합니다.

SASE: 클라우드 네이티브 SASE의 의미는?



- 소프트웨어 중심
- 스케일의 유연성
- 컨테이너/마이크로 서비스
- 글로벌 규모
- 인라인과 스케일
- 싱글 패스 스캐닝
- 단순화, 복잡성 축소
- 멀티테넌트 구조

SSE 솔루션을 선택할 때 고려해야할 7가지 요소

(책자에서 제목만 발취)

1. 성능과 가용성에 따라 확장 가능한 글로벌 클라우드 플랫폼, 운영 검증된 SSE 솔루션 선택
2. 제로 트러스트 아키텍처를 기반으로 구축된 SSE 솔루션 선택
3. 지능적 위협 보호 및 DLP, SSL 트래픽을 규모에 맞게 검사할 수 있는 SSE 솔루션 선택
4. 유연하고 확장 가능하며 다양한 형태의 구축 및 관리 옵션을 지원하는 SSE 솔루션 선택
5. 애플리케이션 연결을 최적화하고 UX 성능을 보장하는 사용자 환경을 제공하는 SSE 솔루션 선택
6. 검증된 에코시스템과의 통합 및 조정이 제공되는 SSE 솔루션 선택
7. 운영 환경 파일럿에서 가치를 쉽게 보여줄 수 있는 SSE 솔루션 선택

지스케일러: 가트너에서 추천하는 디지털 트랜스포메이션 아키텍처

네트워크 보안의 미래는 클라우드(SSE)에 있습니다.

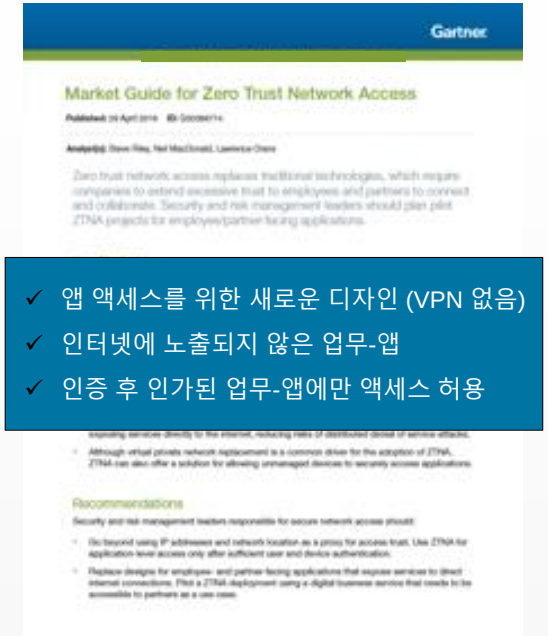

Gartner

The Future of Network Security Is in the Cloud

Recommendations

- ✓ HW 장비 최소화 (라우터/SD-WAN)
- ✓ 클라우드 에지 컴퓨팅
- ✓ 인라인 트래픽 인스팩션 (SSL)

제로 트러스트 네트워크 액세스를 위한 시장 가이드


Gartner

Market Guide for Zero Trust Network Access

Recommendations

- ✓ 앱 액세스를 위한 새로운 디자인 (VPN 없음)
- ✓ 인터넷에 노출되지 않은 업무-앱
- ✓ 인증 후 인가된 업무-앱에만 액세스 허용

"

Gartner®

데이터 센터 중심의 네트워크 보안 아키텍처는 디지털 비즈니스의 다양한 액세스 요구를 처리할 수 없습니다.

Network security architectures that place the enterprise data center at the center of connectivity requirements **are an inhibitor to** the dynamic access requirements of **digital business**.

Zero Trust Exchange

Zscaler Zero Trust Exchange 업계 최고의 보안 플랫폼

150 데이터 센터
글로벌 커버리지

150B+ 1500억/일
리퀘스트 처리

7B+ 70억/일
보안 및 정책 위반 방지

200K+ 20만/일
보안 업데이트

High Authority

Peering: https://www.peeringdb.com

5,000+ 기업 공공 정부, 500+ Forbes G2000, 10년 이상의 플랫폼 운영 노하우, 99.999% 가용성

THE ONLY LEADER: 10년 연속 업계 리더

2020 Gartner MQ for Secure Web Gateways

- 가장 완벽한 비전과 최고의 실행 능력을 보유한 회사
- Secure Web Gateway 는 SASE, ZTNA의 출발점
- Zscaler Zero Trust Exchange 안전하게 디지털 혁신을 가속화

THE LEADER: 최고의 실행 능력

2022 Gartner MQ for Secure Service Edge

- 최고의 실행 능력과 11년 연속 가트너 최고의 리더쉽 선정
- SWG, SSE, ZTNA 세계 최대 규모의 확인된 보안 서비스 클라우드 플랫폼
- Zscaler Zero Trust Exchange 안전하게 디지털 혁신을 가속화

변화의 방향

SASE, ZTNA 도입 검토 목적은?

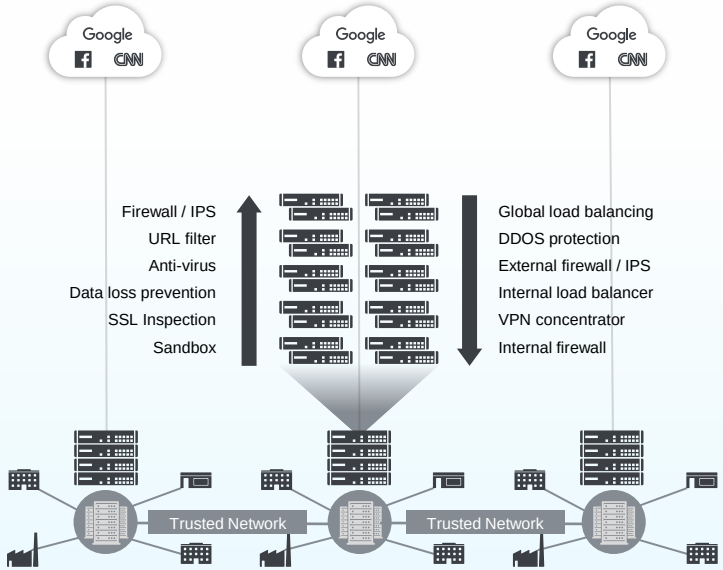
디지털혁신 클라우드 AWS SaaS M365 인터넷 재택근무. Work-From-Anywhere 스마트오피스 생산성 자동화 플랫폼 멀티테넌트 계열사별 정책
SASE. SSE ZTNA. SecureWebGateway. App-control. Next Gen FW. Sandbox. SSL. APT. IPS. VPN. 관제. 유지 보수. 업데이트. 정책관리

보안정책 표준화, WFA/재택근무 지원	• **전사적 보안 혁신** • 모든 임직원 및 파트너까지 조직 표준 보안정책 • 사무실, 재택, 이동 그리고 네트워크에 제한 없는 Secure-Business 환경
투자 보호, 비용 절감	• **지속 가능하고 디지털 비지니스 가속화** • 전용선, 장비 관리, 장비 유지 보수 및 교체 비용 감소 • 클라우드, SaaS 등 기술 변화에 대응
플랫폼: 정책, 운영, 관리	• **플랫폼을 이용한 통합 보안, 운영 자동 관리** • 최신 보안 상태 유지, 비지니스 생산성 보호, 관리 자동화 • 통합 서비스를 통한 자동화와 보안 정책에 의한 운영, 가시성, 감독 강화
SSE/ZTNA 환경	• **SSE 아키텍처로 핵심 서비스 제공** • 보안사각지역 제거, 스케일, 유연성, 서비스 품질 향상, • 사용자 중심의 보안을 플랫폼 서비스로 제공

기존의 구조: 사내 네트워크를 통한 업무 처리

데이터센터 중심

데이터 센터와 네트워크 중심
지점과 데이터 센터 간
전용선을 이용한 연결



사내 네트워크-경계선 기반 보안

중앙 집중식 구조,
네트워크 보안을 통해
이용자와 업무-툴 보호

클라우드 이전의 환경에 적합했던 기존의 구조

클라우드, 인터넷, 원격근무, 디지털 트랜스포메이션

Work From Anywhere
업무 장소 WFA 요구

1.4B 5G 단말
by 2023

서버, IoT, OT 통신량
폭발적 증가

50% of all connected
devices by 2023

클라우드 업무 툴
이용 증가

220x growth
(2016-2021)

인터넷은 기업 업무의
주요 통신 수단

4.6x growth
(2016 – 2021)

임직원 트래픽이 사내 보안통신망의 범위를 벗어나고 인터넷 직접 접속 증가

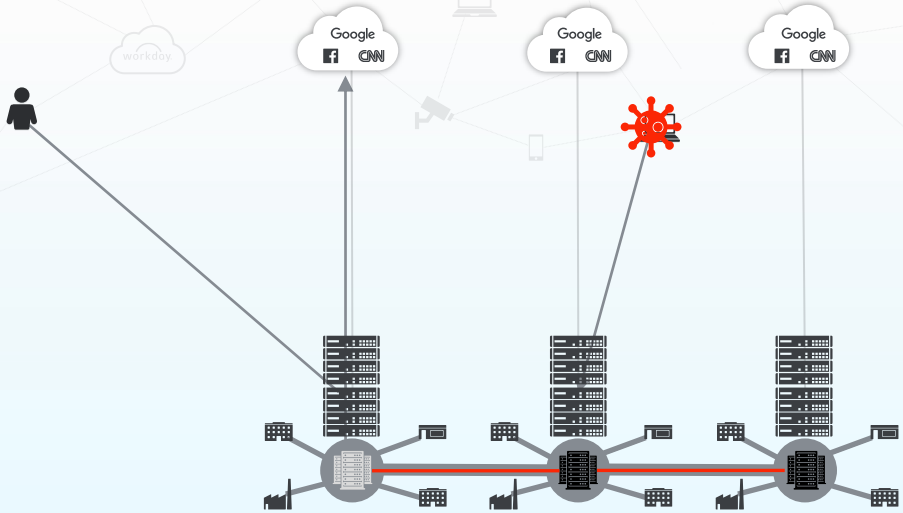
귀사의 현재 네트워크와 보안 아키텍처는 디지털 트랜스포메이션에 대비되어 있나요?

기존의 구조는 디지털 트랜스포메이션을 지연시키고 있다

생산성 감소
Backhauling 트래픽으로 인해 성능 문제가 발생합니다.
(O365/Zoom)

비지니스 리스크 증가
노출된 공격 대상으로 랜섬웨어 및 데이터 손실의 가능성 증가

높은 비용과 복잡성
급증하는 인터넷 트래픽과 사이버 위협은 지속적인 인프라 업그레이드를 요구합니다.



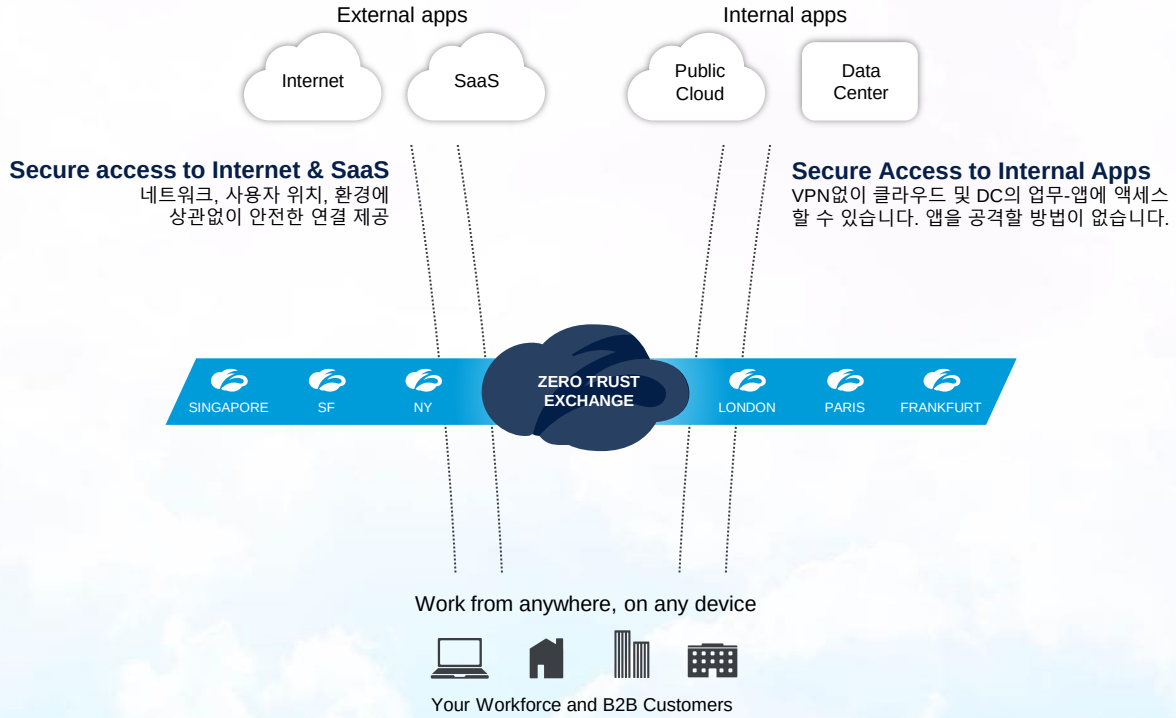
기존의 네트워크와 보안 아키텍처는 지속 가능하지 않으므로 새로운 아키텍처 필요

클라우드 환경을 이끌어가는 3가지 변화

애플리케이션의 변화
DC to Cloud (Agility)

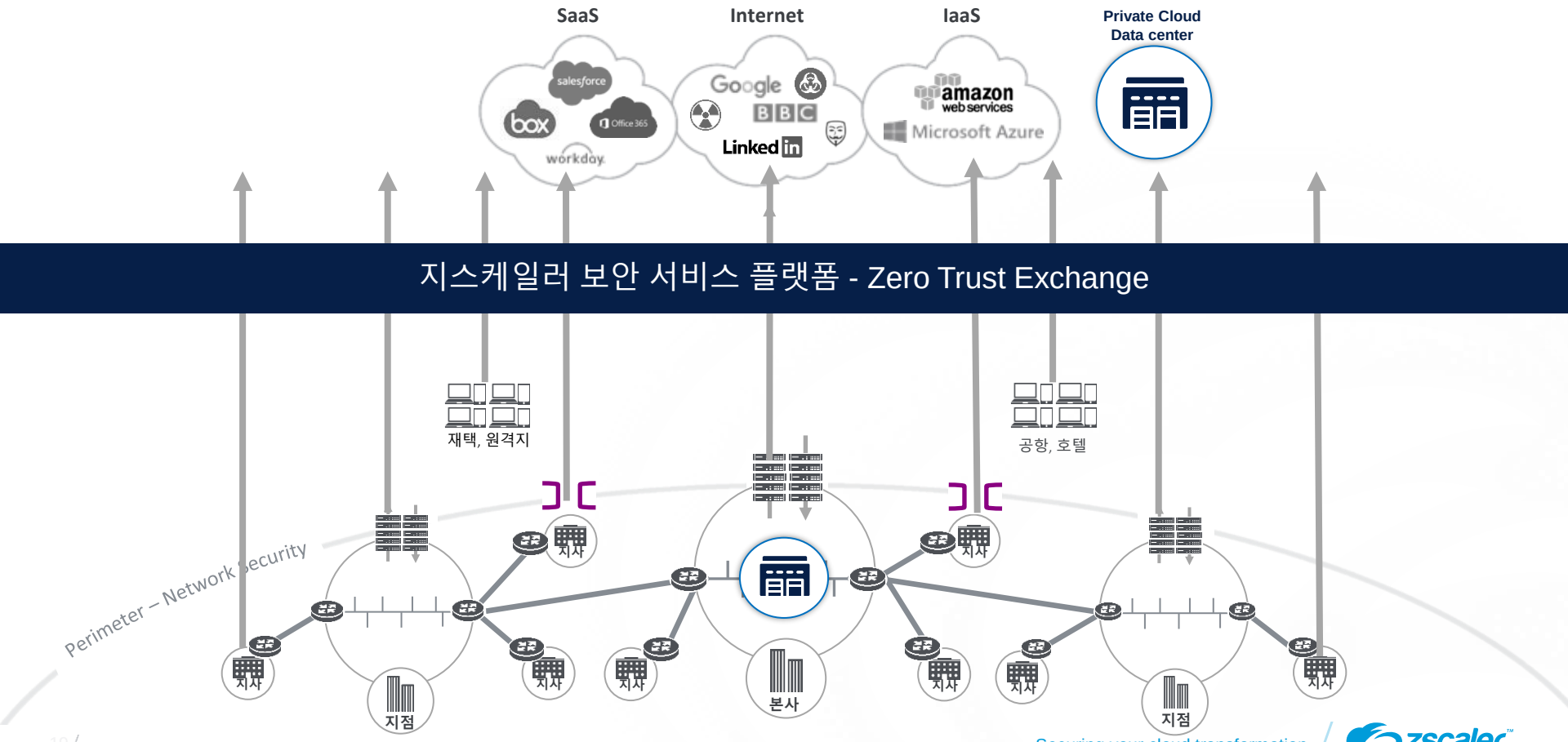
네트워크의 변화
Direct to Internet

보안의 변화
SSE ZTNA



애플리케이션, 네트워크 그리고 보안 변화의 새로운 프레임

변화 하는 환경 – 제로 트러스트 익스체인지 보안 서비스



Zscaler 솔루션

제로 트러스트 익스체인지

솔루션

근무 장소의 한계 극복
1. WFA 보안 환경
2. 사용자 경험 향상

제로 트러스트 보안
3. 사이버 위협 방어
4. 데이터 보호

인프라 구조 개선
5. 지사, 지점 컨넥티비티
6. 클라우드 컨넥티비티

Products

Zscaler Internet Access (ZIA)

Zscaler Private Access (ZPA)

Zscaler Digital Experience (ZDX)

Zscaler Cloud Protection (ZCP)

Services

Threat Protection Engines

DLP Engines

AI / ML Engine

Adaptive Policy Engine

Authentication

Inspection (SSL)

Logging and Reporting

APIs

Zscaler: 4가지 통합된 솔루션

ZIA: Zscaler Internet Access

사이버 프로텍션
데이터 보호(DLP/CASB)
로컬 인터넷 브레이크 아웃 (O365/SD-WAN)

Secure Internet and SaaS access

인터넷 사용

Secure Private App Access

업무-앱 사용

ZPA: Zscaler Private Access

VPN없이 업무-앱 액세스
ZTNA 기반의 DC 액세스 지원
B2B 고객 앱 액세스

ZDX: Zscaler Digital Experience

사용자별 성능 점수, 앱, 위치별 성능 점수
장치 및 네트워크 문제 식별 및 해결

User Experience

사용자의 업무-앱 환경 분석

Secure Apps and Workloads

앱 - 워크로드

ZCP: Zscaler Cloud Protection

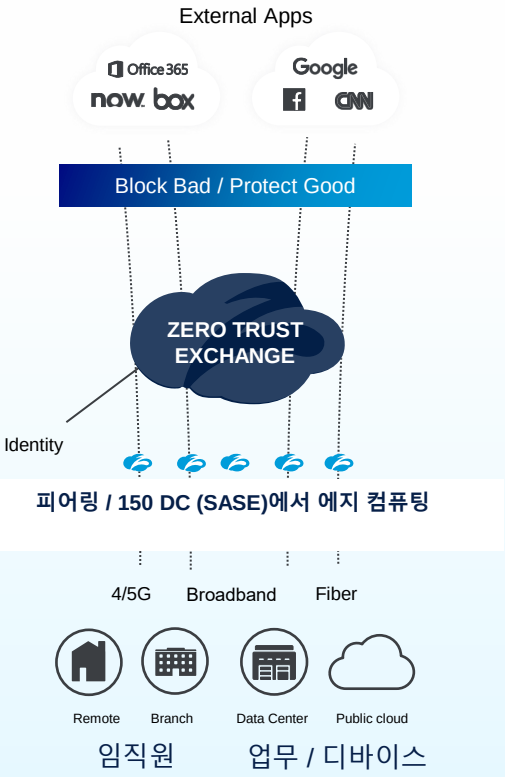
네트워크 세분화가 아닌 앱 세분화
클라우드의 잘못된 구성 해결(CSPM)

글로벌 규모: 150개의 데이터 센터 (SASE)

AI / ML Powered | PolicyNow™ | NanoLog™ | Extensible

통합 서비스와 기존 장비의 한계를 극복, 관리는 편리하게, 비용은 절감

Zscaler Internet Access (ZIA): 안전하고 빠른 인터넷 및 SaaS 액세스



Use Cases

로컬 인터넷 브레이크 아웃

- 150개의 DC에서 시행되는 보안, 피어링(O365 등)
- SD-WAN, 마이크로소프트 통합

사이버 위협 보호

- 정교한 위협에 대한 보호: 랜섬웨어, 피싱, 제로 데이
- 규모의 SSL 검사

데이터 보호

- 사용자, 서버, 장치에 대한 DLP
- SaaS 데이터 보호를 위한 CASB

인터넷에 대한 워크로드

- 인터넷 통신에 대한 보안 워크로드, 서버, IoT 및 OT

비지니스 밸류

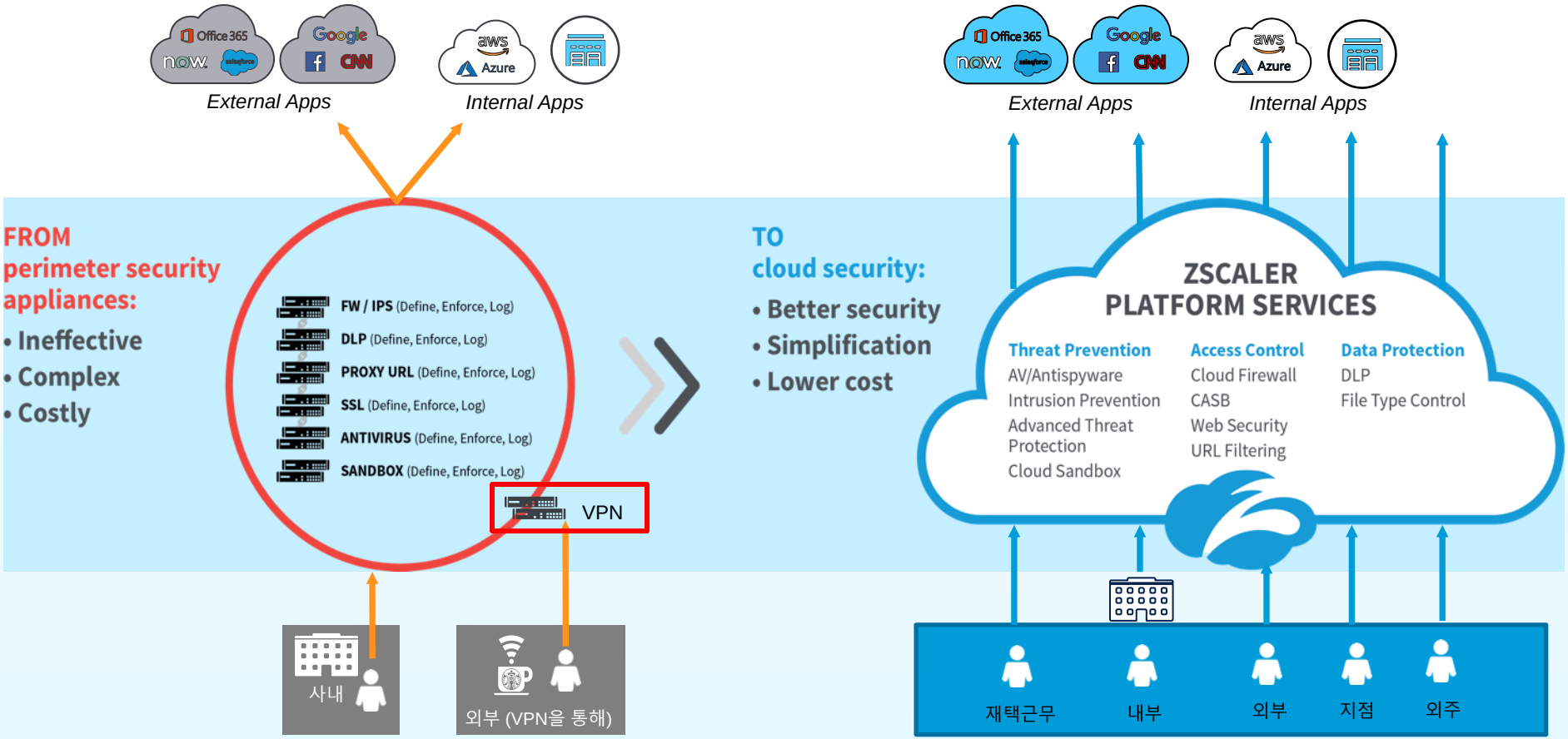
위험 감소 모든 곳에서 동일한 위협 및 데이터 보호

생산성 향상 더 나은 협업과 인터넷 경험

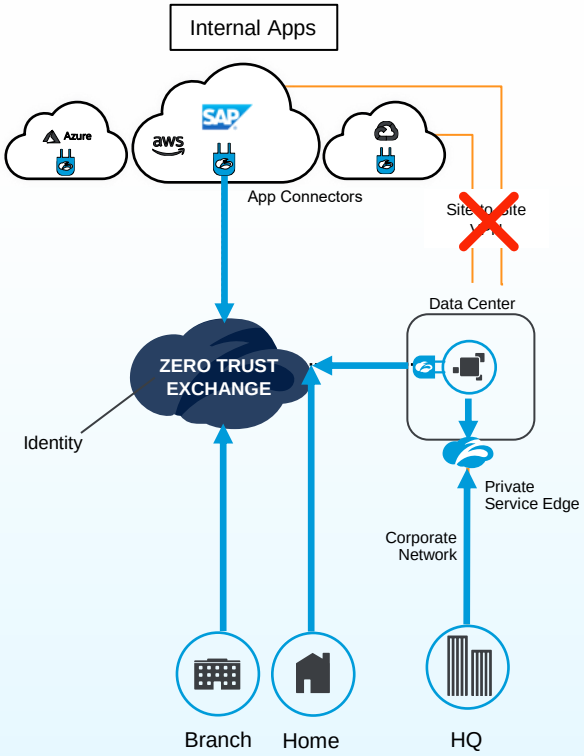
비용 절감 HW 제품 제거, MPLS 비용 절감

- Firewall / IPS
- URL filter
- Anti-virus
- Data loss prevention
- SSL inspection
- Sandbox

Zscaler Internet Access, 제로 트러스트 익스체인지



Zscaler Private Access (ZPA): 안전하고 빠른 내부업무-앱 액세스



Use Cases

VPN 없이 원격 액세스
- 임직원 및 협력 업체에도 원격 보안 액세스 제공
- 앱으로 가는 가장 빠른 경로 – 백홀 없음
- 사용자와 앱 직접 연결, 네트워크 연결하지 않음

퍼블릭 클라우드 앱에 직접 액세스
- 보안 센터를 경유하여 클라우드로 연결하지 않습니다.
- 가상 DMZ의 필요성 제거

온프레미스 사용자를 위한 ZTNA
- 사내와 원격 근무 동일한 환경과 경험 제공
- DC나 사용자 및 업무앱은 동일한 네트워크에 있을 필요 없음

B2B 고객 앱 액세스
- 데이터를 안전하게 유지하면서 B2B 고객 경험을 개선합니다.

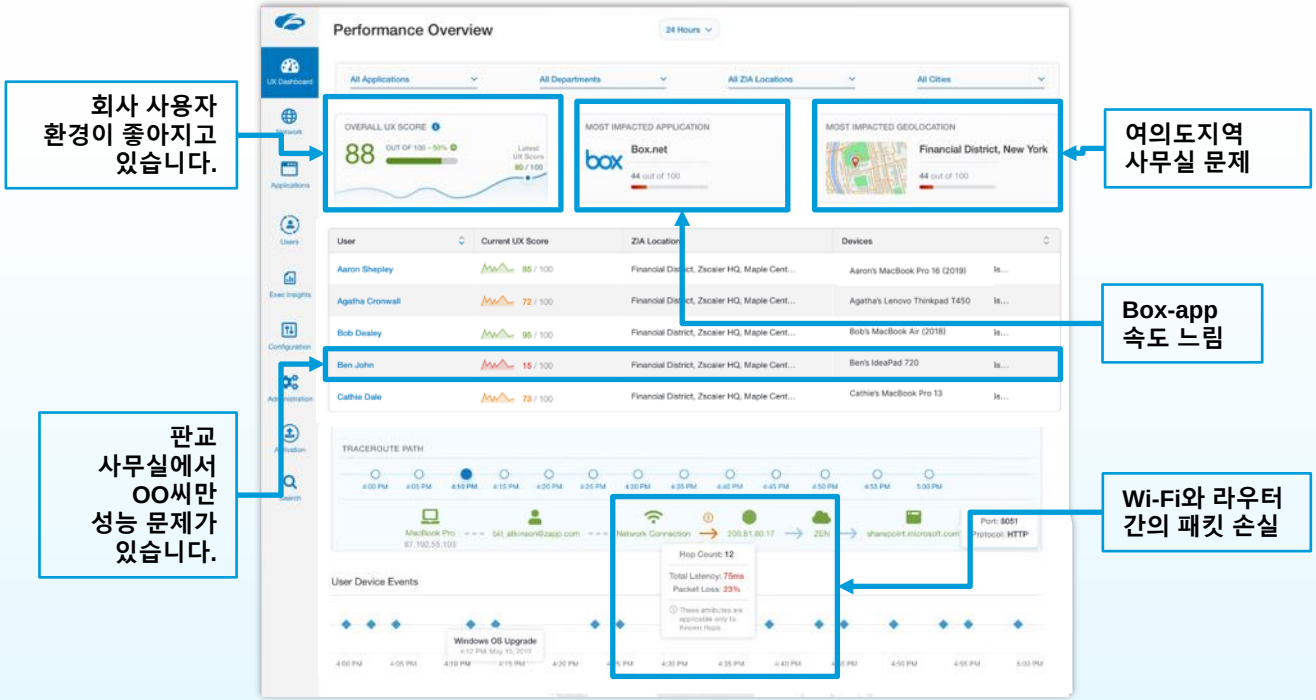
비즈니스 밸류

위험 감소	공격 대상 제거
생산성 향상	SaaS 앱과 같은 개인 앱에 액세스 - 백홀 없음
비용 절감	VPN 인프라 제거

- Global load balancing
- DDOS protection
- External firewall / IPS
- Internal load balancer
- VPN concentrator
- Internal firewall

Zscaler Digital Experience (ZDX): 단말에서 앱으로의 가시성

CEO가 외부에서 O365 성능 문제로 호출할 때
어디서부터 문제 파악을 시작해야 할까요?



WHAT WE DO

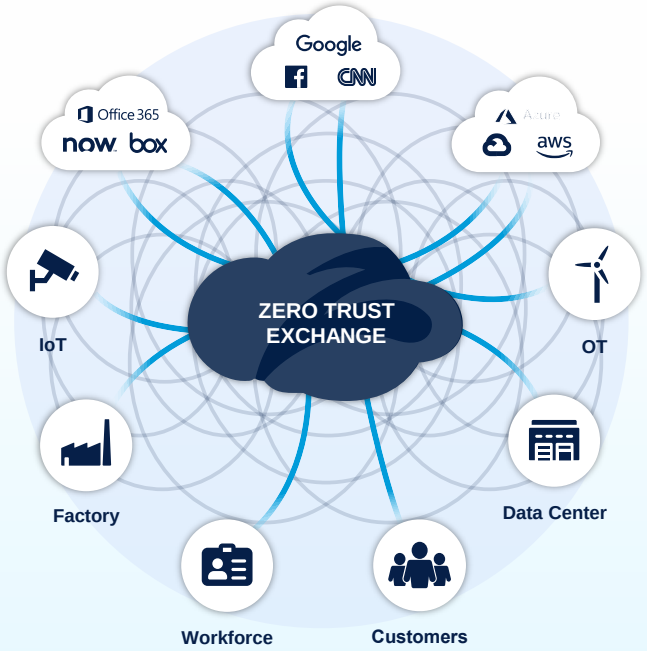
사용자와 디바이스 그리고 업무-앱을 정책으로 관리하고 네트워크에 상관없이 안전하게 연결합니다.

Any-to-Any connectivity**:** User to App, App to App, M2M

OUR MISSION

임직원들이 안심하고 편리하게 사용할 수 있는 클라우드 환경을 제공합니다.

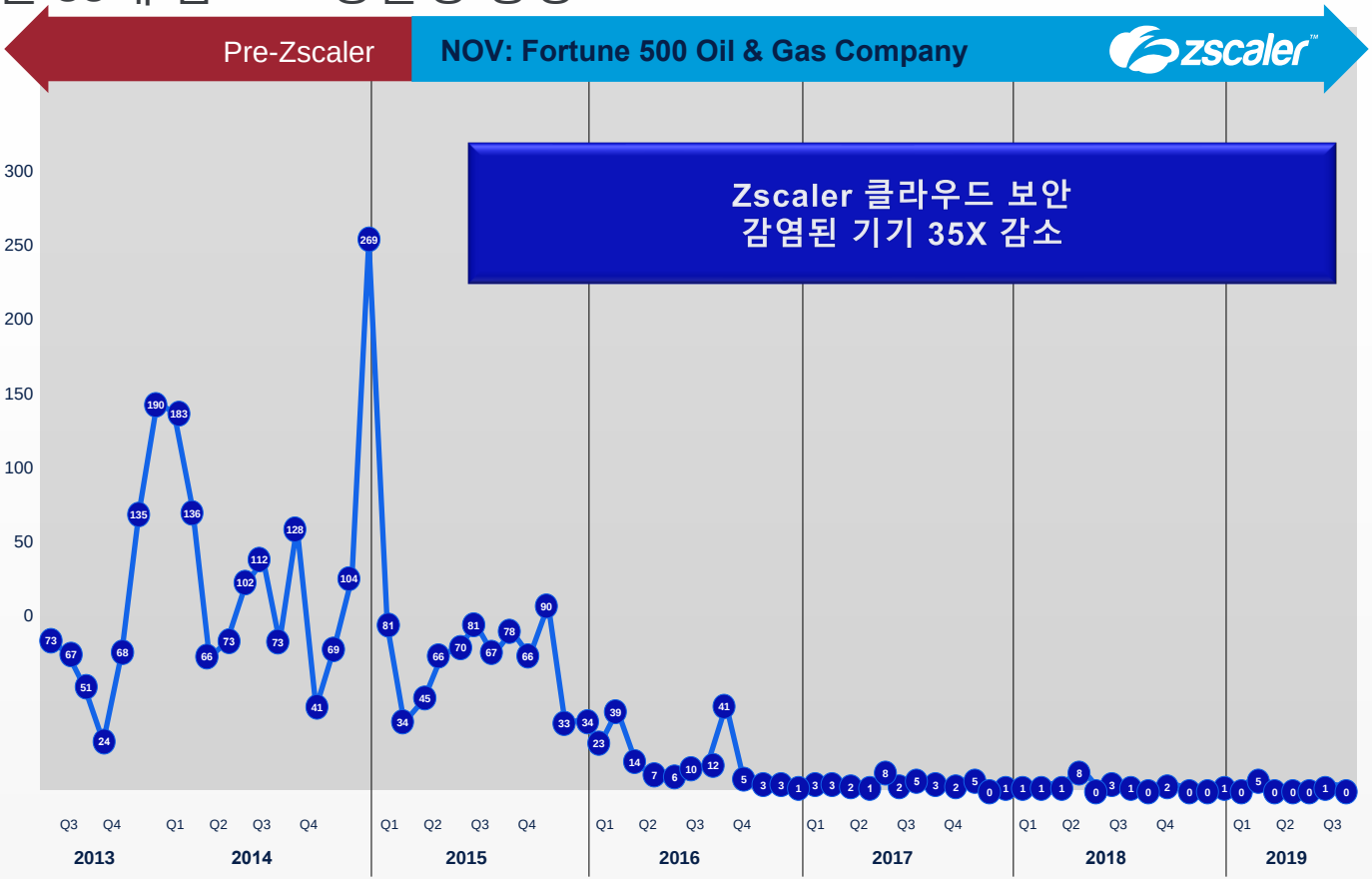
Zero Trust Architecture



기술 파트너 ECO

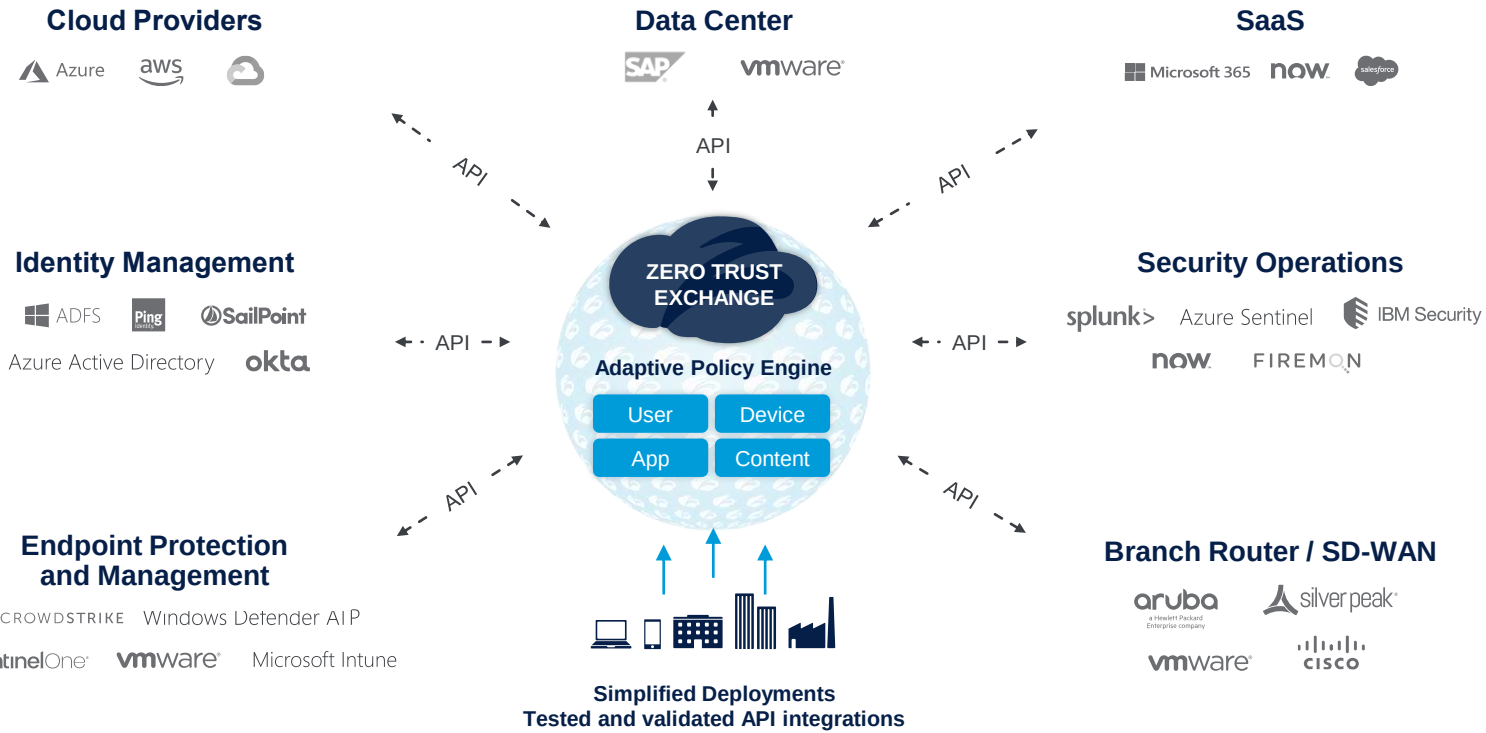
NOV 는 더 나은 위협 제어와 생산성 향상을 이루었습니다.

감염된 단말 35배 감소로 생산성 향상



zscaler

파트너 에코 시스템



분야 최고의 기술력과 협업

혁신적인 파트너십

Microsoft + zscaler™

"샌드빅, 지멘스, GE 등 글로벌 대기업들이 Zscaler와 Microsoft를 사용하여 Office 365와 Azure에서 실행되는 업무-앱들을 더욱 빠르게 제공하고, 다이렉트 액세스 권한을 제공할 수 있게 되었습니다.

안전한 디지털 트랜스포메이션으로 혁신을 선도적인 기업

SIEMENS · KOCH · Micron · GE · L'ORÉAL · ALSTOM · SANDVIK · Johnson Controls

마이크로소프트 보안 20/20 올해의 ISV 파트너

Microsoft 기술과의 혁신 및 통합 우수성

Office 365 네트워킹 파트너

Office 365

가장 빠른 사용자 및 공동 작업 환경을 제공하기 위해 Microsoft에서 인증한 유일한 보안 공급업체

zscaler

MS 주요 통합

Office 365 Azure

Office 365 성능/최적화

Zscaler Internet Access

원클릭 구성
인터넷 익스체인지에서 피어링

클라우드 앱 / 워크로드 보호

Zscaler Cloud Security Posture Management

Identification and remediation
of cloud misconfiguration

Identity Management

ADFS Azure Active Directory

Conditional risk-based
identity access policies

API API

Data Protection

Azure Information Protection
Microsoft Cloud App Security

Zscaler CASB
Zscaler DLP

Visibility and data
protection for cloud apps

Endpoint Protection and Management

Microsoft Intune Windows Defender ATP

Simplified Z-APP deployment
across mobile devices

API API

Security Operations

Azure Sentinel

Log streaming for
threat hunting

Your Workforce and B2B Customers

지스케일러 도입 효과

Value Drivers

사용자 환경 개선

- 전용선 백-홀 제거로 인해 네트워크 대기 시간을 줄입니다. 트래픽은 가장 가까운 Zscaler 데이터 센터로 전송됩니다.
- 인터넷 연결-대역폭 제어를 통해 중요한 업무용 트래픽에 우선 순위 지정
- 피어링을 통한 O365 최적화

운영 효율성

- 인력 투입 시간을 최적화하고 유지 보수를 위한 비용을 절감합니다.
- OS / 펌웨어 업데이트, 패치, 업데이트 주기, 변경 관리 일정 등의 업무 감소
- 플랫폼을 통한 보안, 정책, 관리 자동화

보안 강화 정책 규정 실행

- 보안 정책 및 규정 준수와 실행을 빠르고 쉽게 할 수 있음.
- 랜섬웨어, 피싱, GDPR 및 기타 규정, 맬웨어 및 바이러스와 관련된 위험에 노출 최소화SSL/ TLS를 포함한 모든 트래픽 흐름에 대한 가시성

속도와 민첩성

- 사이트, 지점 사무실, 매장 롤-아웃 및 기타 보안 확대를 위한 프로젝트 활성화 및 가속화
- 장비가 아닌 플랫폼 서비스를 이용하므로 물리적 장벽이 없음
- M&A – 필요한 보안 액세스 및 정책(RBAC) 분석 후 즉시 보안 정책을 통합할 수 있음

비용 최적화

- 아웃바운드/인바운드 인터넷 보안 어플라이언스(SSL, DLP, 샌드박스, ATP) 서비스 통합
- 사용자 트래픽 증가로 인한 HW 교체, 용량 확대 등의 업무 감소
- 네트워크 단순화/ 로컬 인터넷 브레이크아웃 및 클라우드 기반 인프라 서비스

Carbon Footprint / Green

- 기업의 "환경, 사회, 거버넌스" 측정/보고/평가 점수 개선
- 투자자, 주주 및 기타 소비자와 ESG 점수 공유

Zscaler 도입 목적 및 효과

보안정책 표준화, WFA/재택근무 지원	• **표준화된 전사적 보안 정책 수립 및 실행** • 본사, 지점, 재택, 현장, 이동 사용자 영역까지 표준 보안정책 실행 • 지역, 환경을 초월하여 모든 사용자에게 최상의 보안 서비스 제공
투자 보호, 비용 절감	• **반복되는 장비 구매, 업그레이드 및 설치 비용 감소** • 전용선 유지 비용 감소, 관리, 유지 보수 및 교체 비용 감소 • 지속 가능한 보안 서비스 구축으로 투자 보호 및 기술 변화에 대비
플랫폼: 정책, 운영, 관리	• **클라우드 플랫폼을 통한 실시간 통합 자동 관리** • 자동화된 실시간 최신 보안 서비스를 통한 탁월한 위협 탐지 • 간편한 서비스 재구성과 장애 처리, 기능 추가와 정책 설정
SSE/ZTNA 환경	• **완벽한 SSE 아키텍처로 핵심 서비스 제공** • 스케일의 유연성, 싱글 패스 스캐닝, 복잡성 축소, 글로벌 규모의 멀티테넌트 • 사용자 중심의 보안을 플랫폼 서비스로 제공 (11년 연속 업계 리더로 선정)

예제:
귀사의 디지털 트랜스포메이션 로드맵

	1 단계	2 단계	3 단계	4 단계	5 단계
BUSINESS 디지털 혁신					SSE/ZTNA 단순화, 확장성 확보 정책에 의한 통합 관리 최고의 보안 수준 확보
APP ACCESS 클라우드 확대				M365, SaaS 확대	클라우드 우선 정책 임직원 안전하고 편리한 보안 환경 제공
NETWORK 안전한 네트워크			Work From Anywhere	SASE 지점 모델 적용 (Thin Branch Model) 전용선 감소	모든 사용자 가시성 및 분석 정보 확보
SIMPLIFY 물리적 장비 감소		인터넷 보안, VPN 장비 도입 감소	기존 보안 장비와 VPN 축소	기존 VDI 축소 검토 지점 하드웨어 축소	기존 하드웨어 철수 솔루션 단순화 (통합 관리, 통합 가시성)
SECURE SSE 도입 보안 플랫폼 서비스	Zscaler ZIA 도입	ZIA 사용자 및 ZPA (ZTNA) 확산	Zscaler ZIA/ZPA Sandbox, ATP, Advd FW, CASB	Zscaler CSPM Data Protection, ZDX 확산	SSE, ZTNA 완성

안전한 디지털 혁신을 위해 Zero Trust 로 비즈니스를 강화하고 새로운 결과를 달성할 수 있습니다.

생산성 향상

가장 빠른 경로
(백홀 없음)

Enforce policy close to the user in 150 data centers

위험 완화 및 제어

정교한 위협으로부터 보호
(랜섬웨어/피싱)

Data loss prevention for users, IoT, and servers

비용과 복잡성 감소

통합 보안을 제공하고, 기능별 보안 장비 감소

Reduce MPLS costs

비즈니스 민첩성 증대

새 사이트를 빠르게 스핀업
(인터넷 연결)

M&A IT 통합 시간을 월에서 일 단위로 가속화

"더 안전하고, 더 나은 서비스를, 더 낮은 비용으로 운영 할 수 있다는 것은 드문 경우 입니다." (It's a rare occasion in history where it got more secure, better, and cheaper all at once.)

보안 정책, 서비스 운영의 방향

- Dashboard- Demo
- CIO 보고서
- CISO 보고서
- 분기 보고서

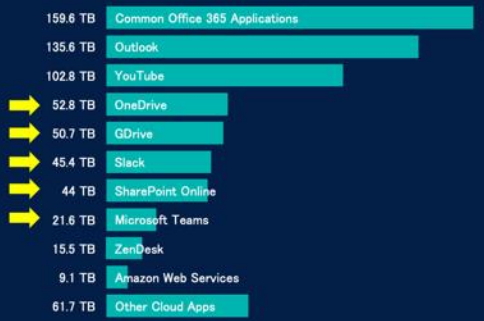
Value Summary 예제

Your Top Cloud Applications

Common Office 365 Applications uses 12.5% of your total bandwidth and Common Office 365 Applications was your top cloud application in the previous quarter.

Top Cloud Applications This Quarter

By Allowed Bytes



50%

Percentage of bandwidth your top 10 cloud application(s) account for.

Your Top Productivity Apps

Your productivity applications use 14.9% of your total bandwidth.

Top Productivity Applications

By Allowed Bytes

Traffic Volume -

Quarterly Comparison

By Bytes

Your Office 365 Growth

Total Office 365 traffic was 844.4 TB in the last 6 months, decreasing 1% over the period

Top Office 365 Applications

By Bytes

Traffic Volume -

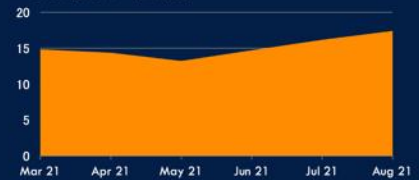
Quarterly Comparison

By Bytes

Traffic Trend for Office 365 Applications – Last 6 months

Outlook (In TBytes)

Sharepoint (In TBytes)

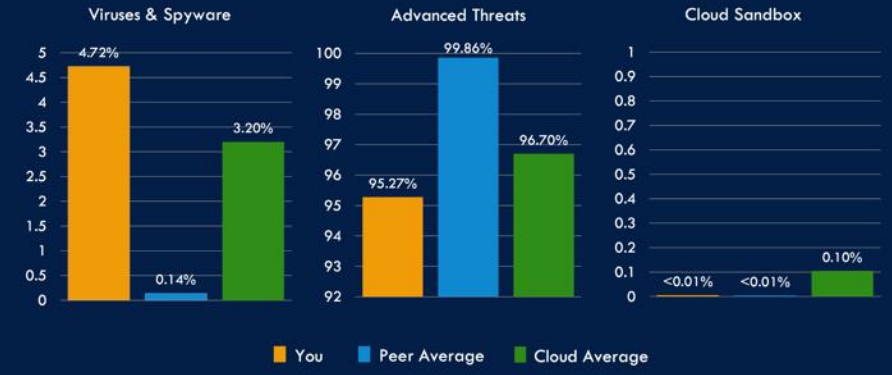


Microsoft Teams (In TBytes)

Skype (In TBytes)

Threats Blocked by Threat Category

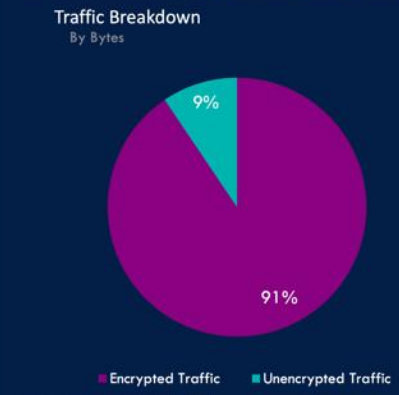
Breakdown of the 610.9 Thousand threats blocked last quarter



Compared to Other Customers where Industry is Retail & Wholesale, Geography is Other and Size is 10001-25000

Protection Against Threats in Encrypted Traffic

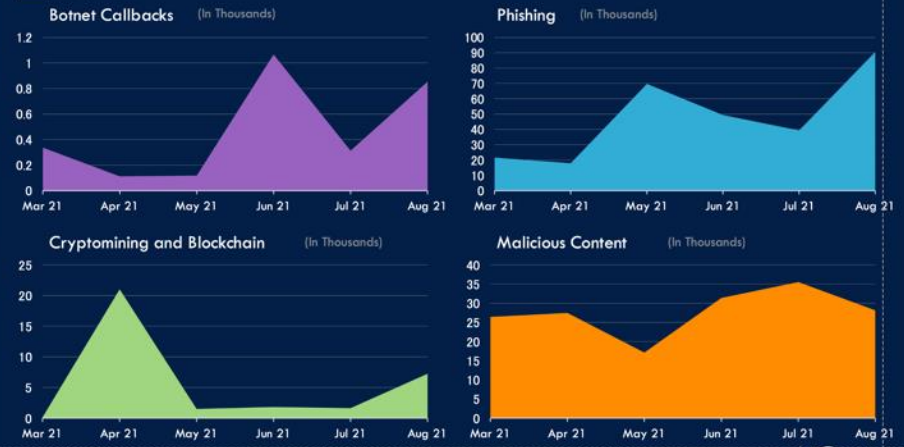
Sophisticated threats are often hidden in encrypted traffic. As a proxy architecture, Zscaler is designed to scan this traffic for security and DLP.



Cloud Sandbox (Advanced)

20,429 files were sent to Sandbox for analysis by [redacted]

Summary of Advanced Threats Blocked (Transactions)



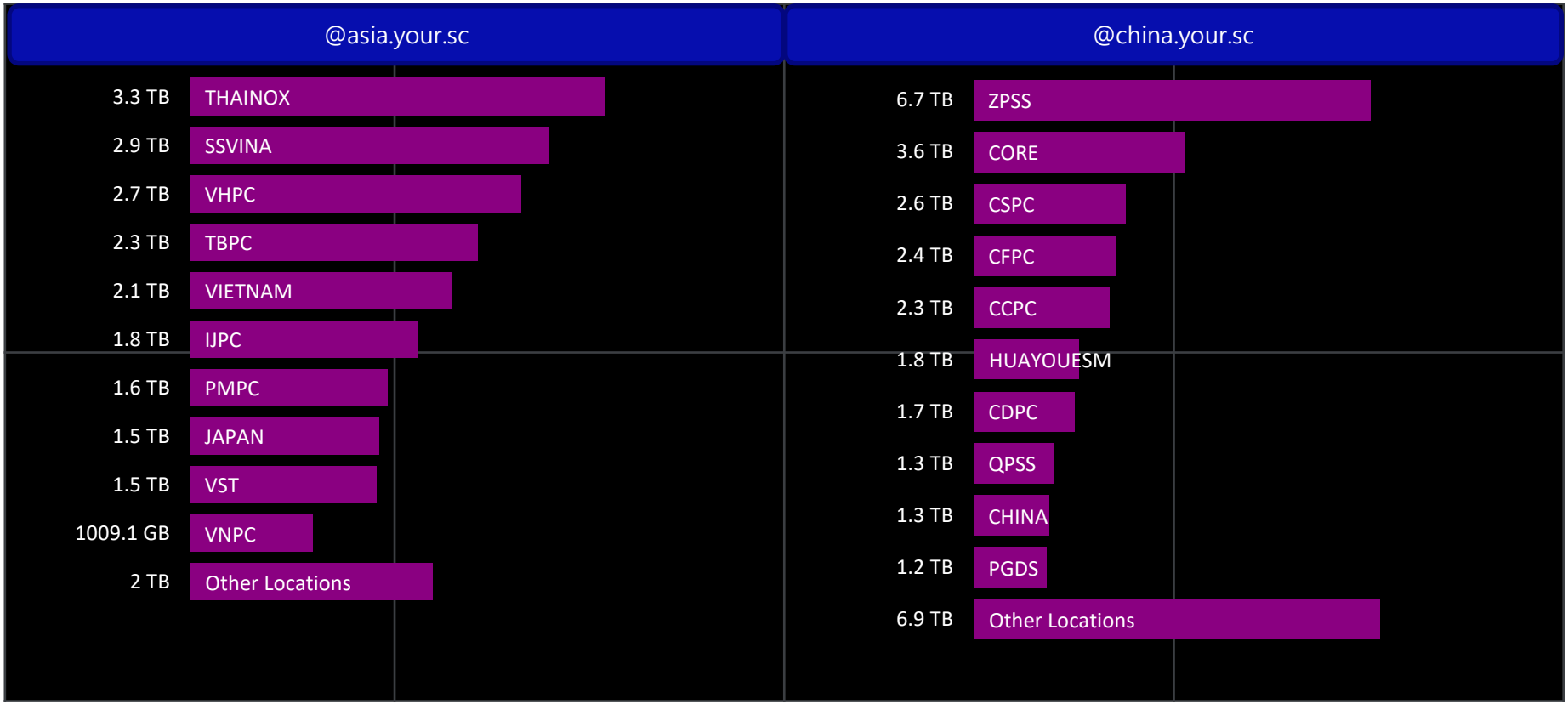
예시: 귀사의 도메인 별 Zscaler 구성 현황

도메인	@china .your.sc	@office .your.sc	@westasia .your.sc	@asia .your.sc	@america .your.sc	@mexico .your.sc	@global .your.sc	@eu .your.sc
Org-ID	xxx6057	xxx1737	xxx20526	xxx88603	xxx20582	xxx0741	xxx1478	xxx63885
Licenses 수	2188	1600	899	1878	4500	200	2550	1900
Traffic Forwarding	GRE+Agent	GRE+Agent	GRE+Agent	GRE+Agent	GRE+Agent	GRE+Agent	Agent Only	GRE Only
Authentication	GRE - Non Auth Agent - SAML	GRE - Non Auth Agent - SAML	SAML (Okta)	GRE - Non Auth Agent - SAML	GRE - Non Auth Agent - SAML	GRE - Non Auth Agent - SAML	SAML (Okta)	Non Auth

총 35,000 User License

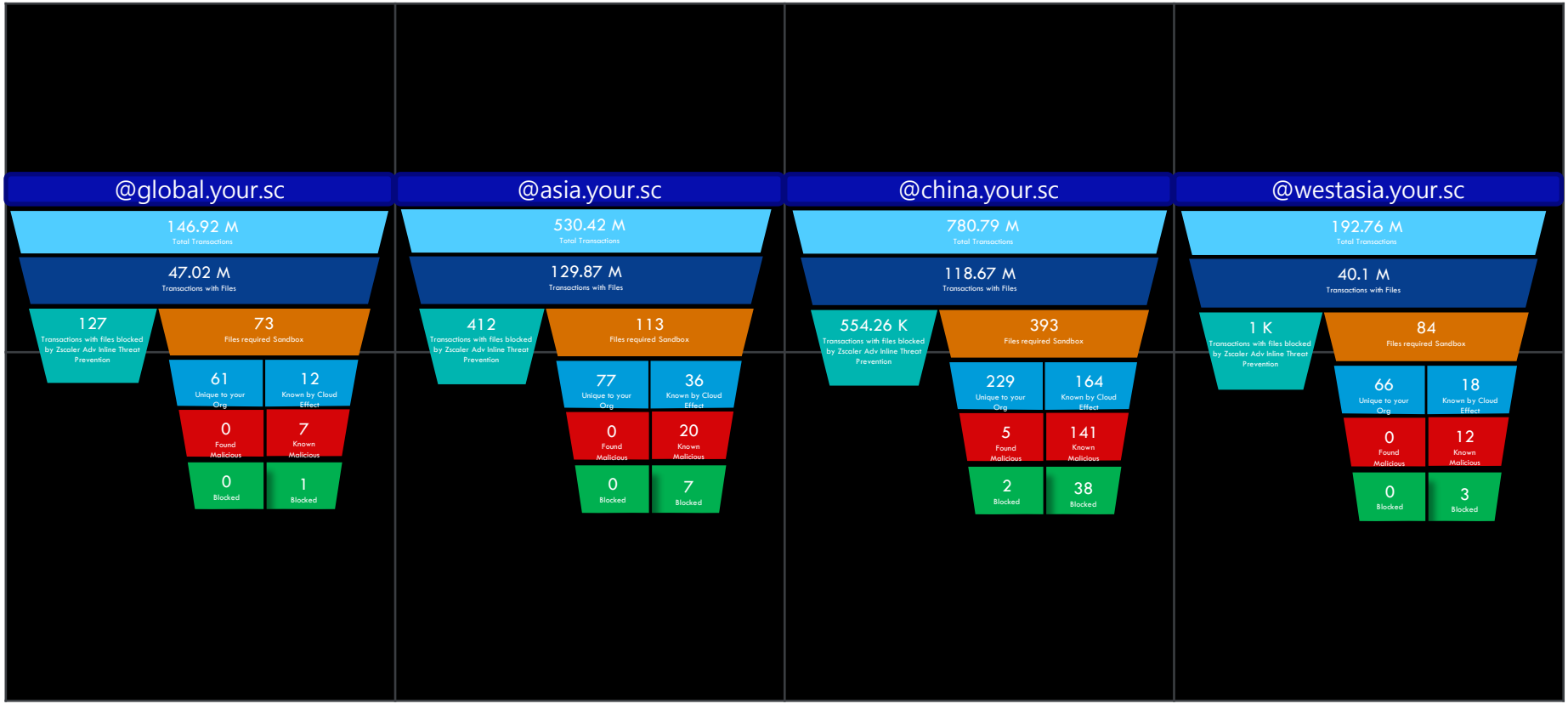
도메인 별 지점 트래픽 사용 현황

- 각 도메인내 Location으로 분류된 지점 별 2분기 대역폭 사용 현황 리포트(Agent 기반의 사용자 트래픽은 제외)



도메인 별 SandBox 분석 현황

- 도메인 별 전체트랜잭션과 File다운로드 트랜잭션 Sandbox 분석이 진행된 트랜잭션 값을 표기한 리포팅



Cloud Application 사용 현황

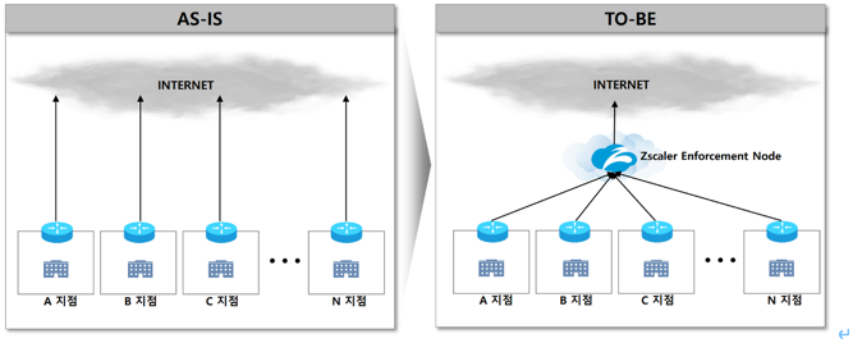
- 도메인 별 전체 Web Application 현황 정보이며 Productivity, Collaboration, Streaming App 등 전체 Application Top10에 대한 정보를 표기

Case

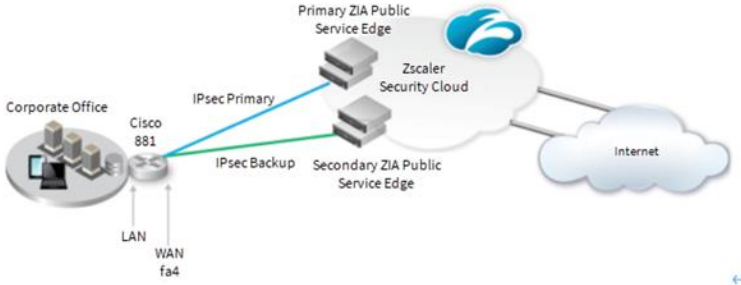
기업 A: 국내 및 해외 다수의 대/중/소 규모 지점, 보안 표준화

- 구축 개요
  - 국내 A 사는 전세계 많은 지점을 보유하고 있으며, 지점별 근무 인원이 많게는 100 명 이상부터 적게는 10 명 이내의 소규모 지점 운영 중임.
  - 기존 온프레미스 형태의 보안 장비로는 국내 본사 근무자들에게 적용하고 있는 보안 서비스를 해외 지점에 근무하는 사용자에게 동일하게 적용하기 어려움(비용문제, 운영관리문제 등).
  - 온프레미스 형태의 장비 구매 없이 다수의 지점에서 동일한 보안 서비스를 받으면서 사용자 기반의 과금 체계를 제공하는 클라우드 기반의 보안 서비스가 필요하게 되었고 이에 Zscaler 를 검토하여 도입함.

- 구축 및 운영
  - 전 세계 지점 도입에 앞서 소규모 지점이 다수 존재하는 국가에 우선 도입이 결정되었다. 기존 인터넷 사용시 안티바이러스 백신 외에는 보호받지 못한 사용자 인터넷 트래픽을 현지 지점에서 가장 가까운 Zscaler 데이터 센터로 연결하여, 약 60 여개의 소규모 지점들이 기존에 적용 받지 못했던 많은 보안 서비스를 전 지점에 일관성 있게 구축했다.



<Zscaler 서비스 전환 후 네트워크 구성>



<Zscaler IPsec 구성>

- 또한 IPSec Tunnel 은 이중화 형태로 구성하여 Zscaler 데이터 센터에 이상이 발생할 경우, 라우터의 Health Check 를 통해 라우팅이 자동으로 전환되도록 구성하여 사용자들에게 발생할 수 있는 서비스 단절을 최소화 하는 안전한 Backup 서비스를 마련했다.

도입 후 개선 효과

- A 사에서는 Zscaler 를 도입함으로써 많은 투자비용을 절감하고 보안 장비 설치로 인한 인력 부족에 의해 주요 사업장에만 적용될 수 밖에 없는 관제를 소형 지점에도 확대 적용하여, 복잡해진 인터넷 위협에 대비한 차세대 통합 보안을 적용 받을 수 있게 되었다.
- 지속적으로 늘어나는 보안의 필수 요소인 HTTPS(SSL) 트래픽에 대한 SSL Inspection 을 적용하여 인터넷 트래픽에 대한 관제 한계를 극복했다.
- 개별 장비의 분산 운영으로 발생되는 무분별한 예외 처리, 기업 보안 정책 수준 위반에 대한 글로벌 통제 문제를 해결했다.
- 관리자의 경우에는 기존의 특정 네트워크에서만 가능했던 관리의 제약에서 벗어나, 재택근무 및 출장 중에도 언제 어디서라도 접속할 수 있는 Zscaler 관리 포탈을 통해 Zscaler 서비스를 적용 받고 있는 모든 지점의 보안 상태를 모니터링하고 정책을 제어하는 것이 가능해졌다.

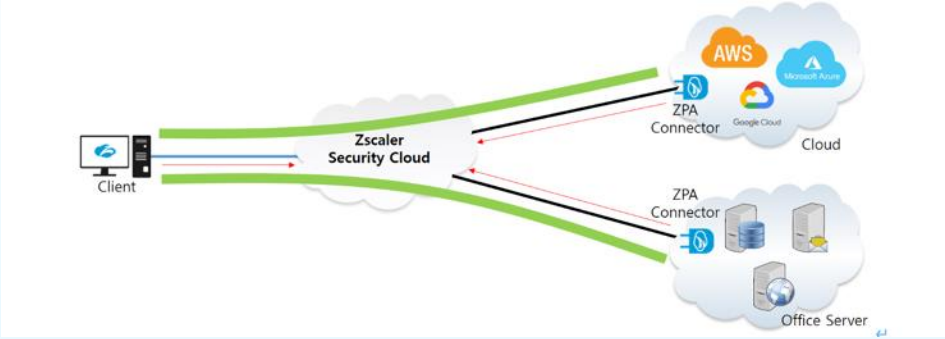
기업 B: 지역별 대형 사업장, 클라우드, 스마트 오피스, WFA

전직원 ZIA 사용, 필수 인원 ZPA 사용 중인 고객, ZPA를 전 직원으로 확산, VPN에서 탈출

- 구축 개요
  - 국내 B 사는 대부분의 업무 관련 서버들이 AWS 와 같은 클라우드에 위치
  - 재택근무가 많은 관계로 클라우드에 접근하는 직원들의 IP 가 매번 다르며 이와 같은 이유로 클라우드 접근에 대한 보안 적용이 어려움

- 구축 및 운영
  - 직원들의 클라우드 접근에 대한 보안을 강화하기 위해 Zscaler ZPA 를 도입하게 되었다.
  - 기업이 사용하고 있는 클라우드 내에 ZPA Connector 를 설치하여 직원들이 클라우드 접근 시 ZPA Connector 를 통해 클라우드 내의 서버에 접근이 가능하게 되었다.
  - 클라우드 접근에 대한 ACL 정책에 ZPA Connector IP 를 등록하여 ZPA Connector 만 접근 가능하도록 설정했다.

- 도입 후 개선 효과
  - 기존 재택근무로 인하여 클라우드 접근 통제에 대한 정책 적용에 어려움이 있었으나 ZPA 도입 이후 모든 사용자는 ZPA Connector 를 통해 접근하기 때문에 클라우드 접근 ACL 에 ZPA Connector IP 등록만으로 손쉽게 보안 정책 적용이 가능하게 되었다.
  - ZPA 정책을 통해 각 사용자마다 접근 가능한 서버들을 다르게 적용, 최소한의 접근 권한만을 부여하여 보안 정책을 강화하였다.



문의 / zerotrust@bespinglobal.com

BESPIN GLOBAL

HELPING YOU ADOPT CLOUD.