# 업무환경 변화에 따른 클라이언트 보안 전략

(주)엑스퍼넷

전략기술부 김일권 프로

# 금융권의 IT 업무 환경 변화 과정

## 재택근무와 외부에서 사내 시스템 접속이 가능하도록 지침 변경

□ 외주 직원도 재택근무 가능함

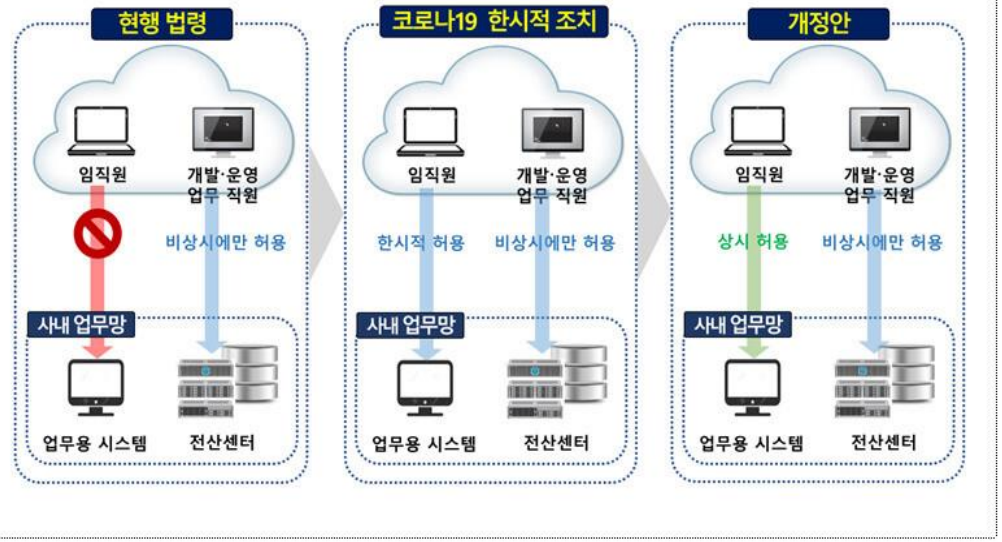
○ 『전자금융감독규정시행세칙』(이하 '시행세칙') 제2조의2 제1항 제2호는 모든 사내 업무용 단말기*에 대해 적용되므로 단말기 사용자의 소속에 따라 달리 적용되지 않음

* 「전자금융감독규정」 제15조 제1항 제3호의 내부통신망과 연결된 내부 업무용 시스템

4. IT직원이 개발·보안·운영 업무가 아닌 이메일, 그룹웨어 등의 업무시스템 사용 목적의 원격접속은 가능한지?

□ IT직원도 개발·보안·운영 업무가 아닌 이메일, 그룹웨어 등의 업무 시스템 사용을 목적으로 원격 접속하는 것은 가능함

<재택근무 관련 망분리 제도 개선사항>

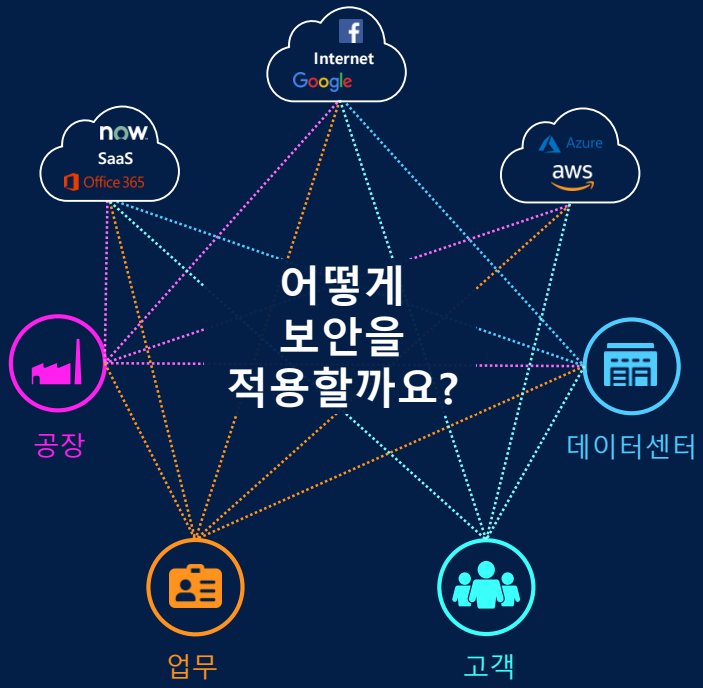



출처 : 금융감독원

# 디지털 트랜스포메이션은
# 선택이 아닌 필수 과정

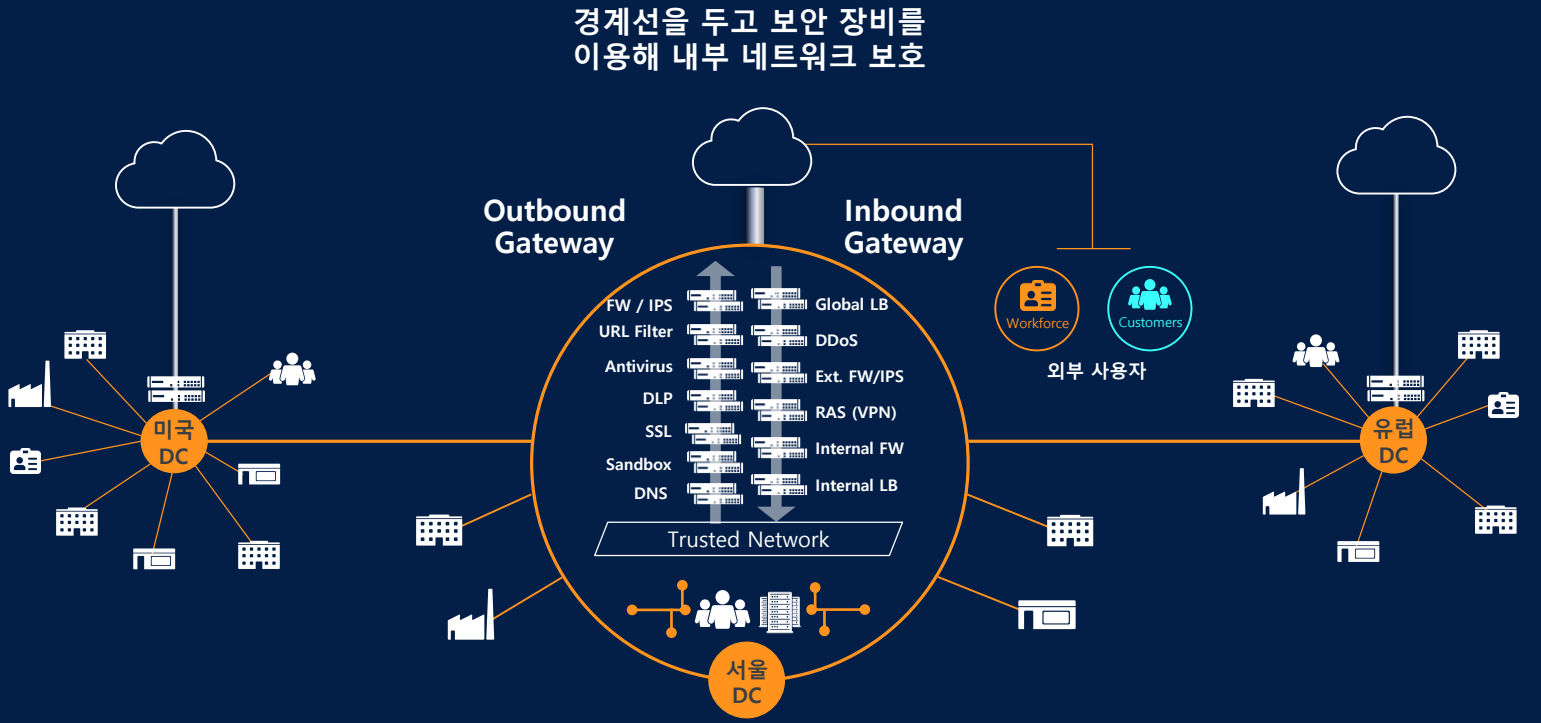
## 많은 분야에서
## 디지털 트랜스포메이션이 일어납니다.

- **클라우드** | 신속, 규모, 협업
- **모빌리티** | 이동성, 생산성
- **IoT / OT** | 운영적 효율성
- **인터넷** | 연결



# 과거 이 모델은 보안 역할을 충분히 만족

## 내부 네트워크를 통하여 사용자와 데이터센터의 업무 앱을 연결



# IT를 통해 비지니스 생산성 극대화

**애플리케이션 트랜스포메이션**
데이터센터 -> 클라우드

용이한 협업
새로운 비지니스 모델
심플한 IT

**시큐리티 트랜스포메이션**
네트워크보안 -> SASE

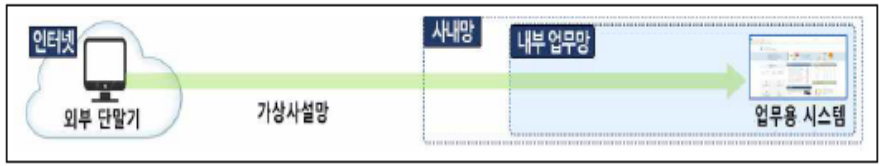
정책기반
투명성
표준화

**네트워크 트랜스포메이션**
WAN -> 인터넷

빠른 사용자 경험
네트워크 비용 감소
심플한 IT (신속대응)

# 내가 근무하는 모든 곳이 “오피스”

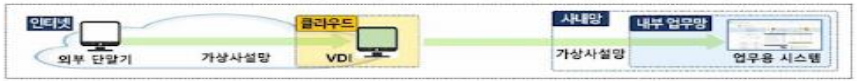
< 직접 방식의 예시 >




< 간접 방식의 예시 >

❶ 내부망과 분리된 원격접속 전용 VDI를 경유하여 내부망에 접속


❷ 클라우드에 있는 원격접속 전용 VDI를 경유하여 내부망에 접속




❸ 내부망에 위치한 업무용 VDI로 접속


❹ 원격접속 프로그램을 통해 내부망 업무용 단말기로 접속


## 접속 방식에 따른 보안 통제사항 비교

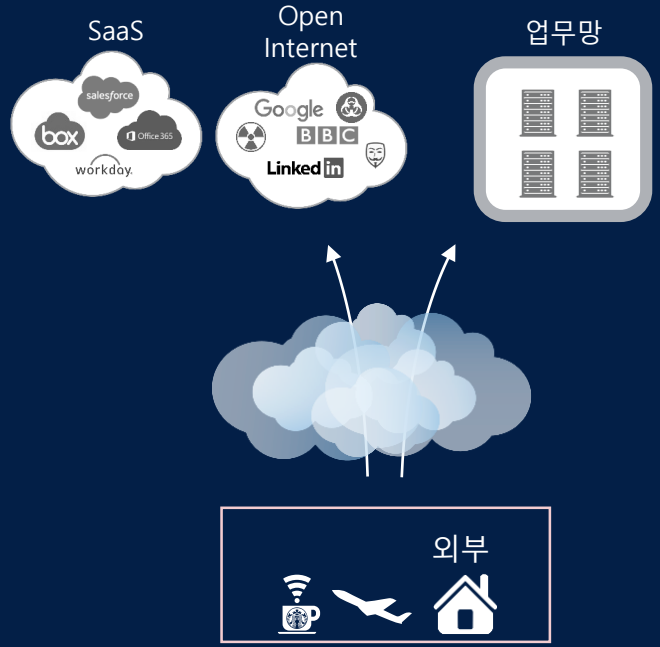
| 보안정책 | 직접 연결 | 간접 연결 |
|---|---|---|
| 허용되는 단말기 종류 | 회사 지급 단말기만 가능 | 개인 단말기도 가능 |
| 인터넷 차단 | 항상 차단 | 업무망 연결시 차단 |
| 백신 설치, 최신 운영체제 유지, 비밀번호 설정 | 사내 근무시와 동일 | |
| 파일 송수신 | 허용 | 차단 |
| 단말기 설정 변경, 외부저장장치 사용 | 차단 | 허용 |
| 내부 전산자료 출력, 화면 캡쳐 | 차단 | 차단 |
| 내부 전산자료 저장 | 암호화 저장 | 차단 |

그래픽=유상연 기자 prtsy201@ BUSINESS watch

출처 : Business Watch

# 성공적 클라우드 도입을 위해서는 클라우드 기반의 아키텍처 필요

내 PC로 **인터넷** 과 **내부 망접속**
을 할 수 있는 환경




데이터센터,
HW 기반

Azure

업무 앱

workday.

salesforce

네트워크 보안

zscaler™

# Zscaler, 안전한 인터넷과 클라우드 환경

모든 클라우드
모든 네트워크
모든 사용자
모든 지역

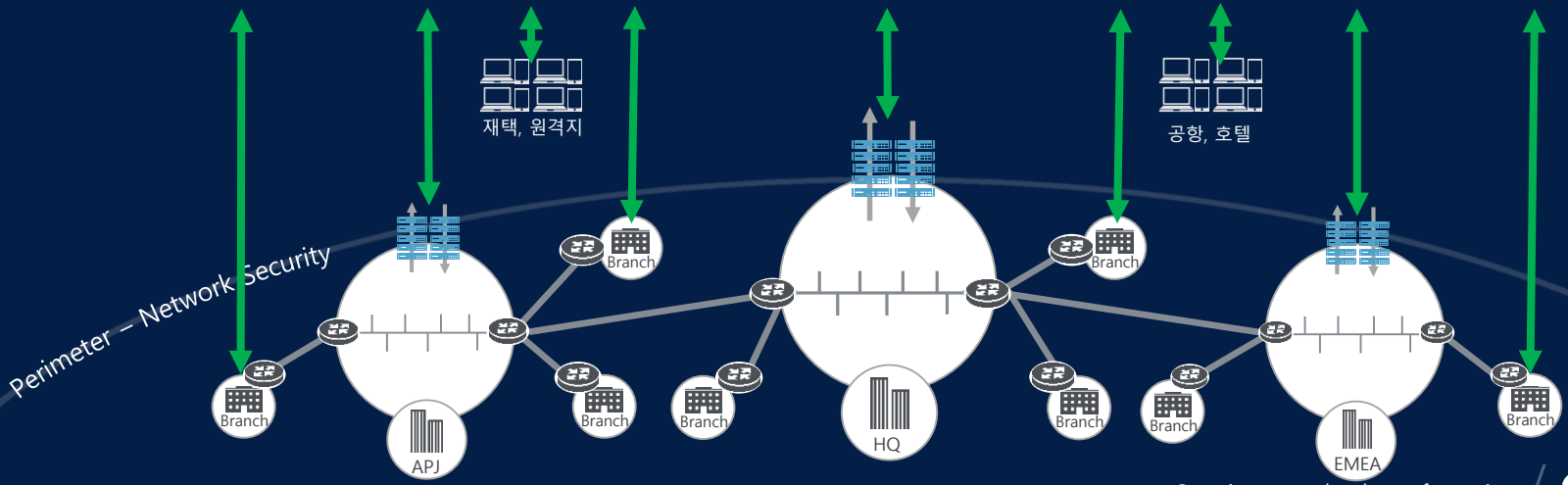
SaaS

Open Internet

IaaS

종속되지 않는
새로운 관점의
사용자 보안 정책

지스케일러 보안 플랫폼 (전 세계 150개 데이터 센터)



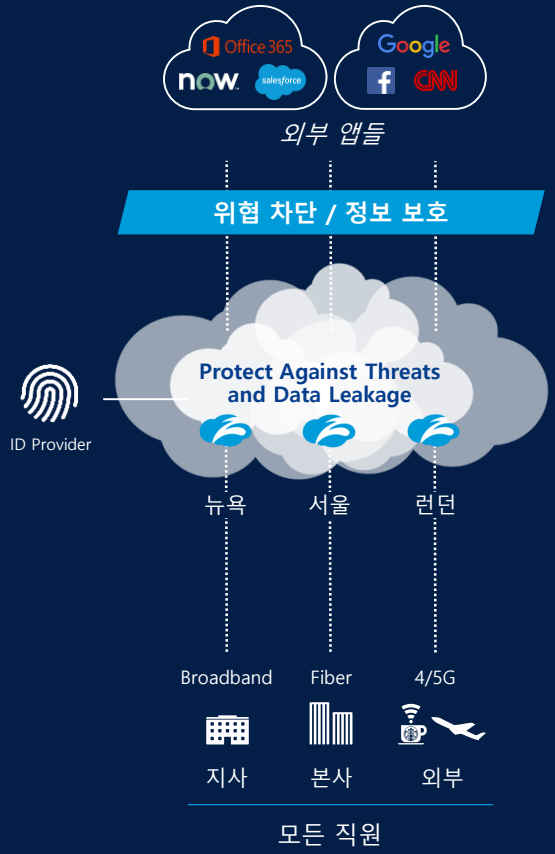



Securing your cloud transformation

# 안전하고, 빠르고, 신뢰할 수 있는 앱/데이터 접속 제공

# ZIA(Zscaler Internet Access)

# Zscaler Internet Access: 안전하고 빠른 인터넷과 SaaS 이용




## 사용 사례

### Office 365

- 업무앱의 우선 순위와 MS peering 제공
- One-click 설정 제공

### Secure SD-WAN

- 지점 지사의 현지 direct-to-internet 환경
- SD-WAN 제조사들과의 API 인테그레이션

### 위협 차단

- 용량 한계를 극복한 Encrypted traffic 검사
- 클라우드 효과, 확인되면 즉시 반영

### 데이터 보호

- Shadow IT discovery
- Protect IP / PII / Compliance

**표준화 • 복잡성 제거 • 동일한 보안 정책 실행 (이동, 지사, 본사)**

## 플랫폼 서비스

### Threat Prevention

Proxy (Native SSL)
Advanced Threat Protection
Cloud Sandbox
DNS Security

### Access Control

Cloud Firewall
URL Filtering
Bandwidth Control
DNS Resolution

### Data Protection

Cloud DLP
Exact Data Match
CASB
Browser Isolation

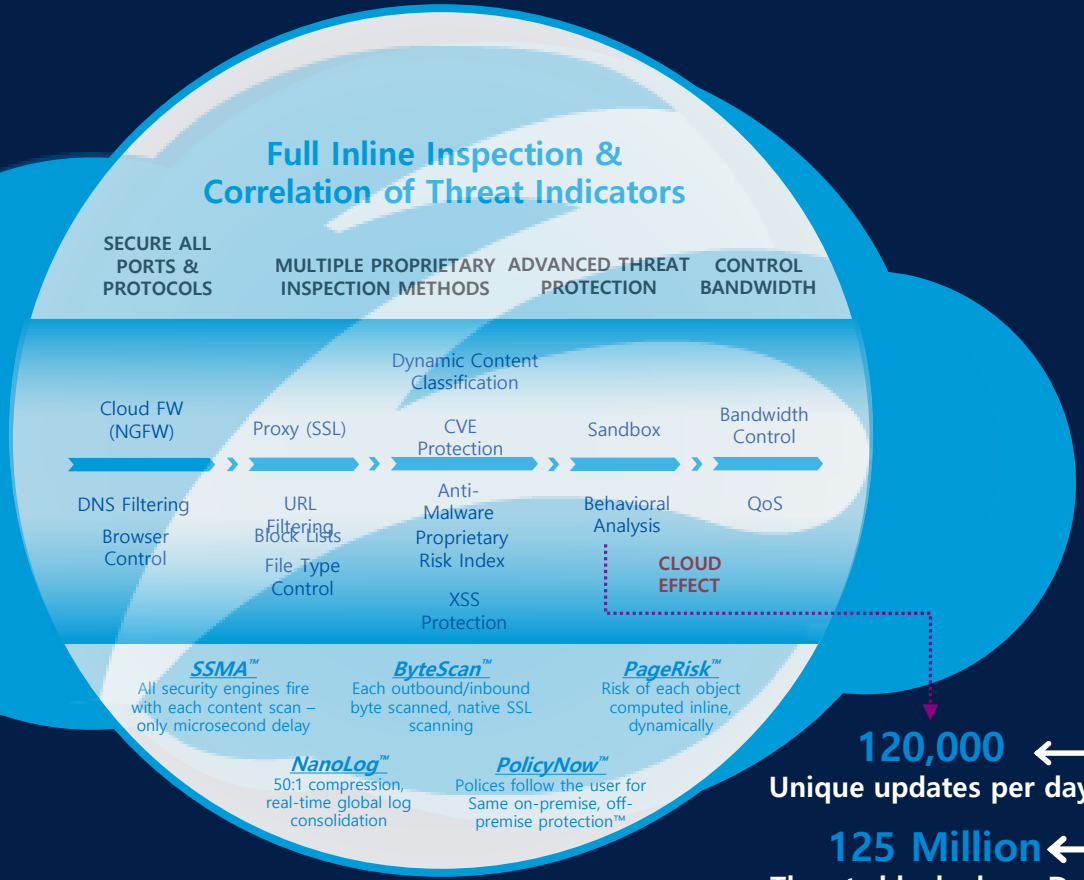


Securing your cloud transformation

zscaler™

# Zscaler Internet Access: 안전하고 빠른 인터넷과 SaaS 이용

**80 Billion**
Requests per Day




**120,000** ← 60+ threat feeds
**Unique updates per day**

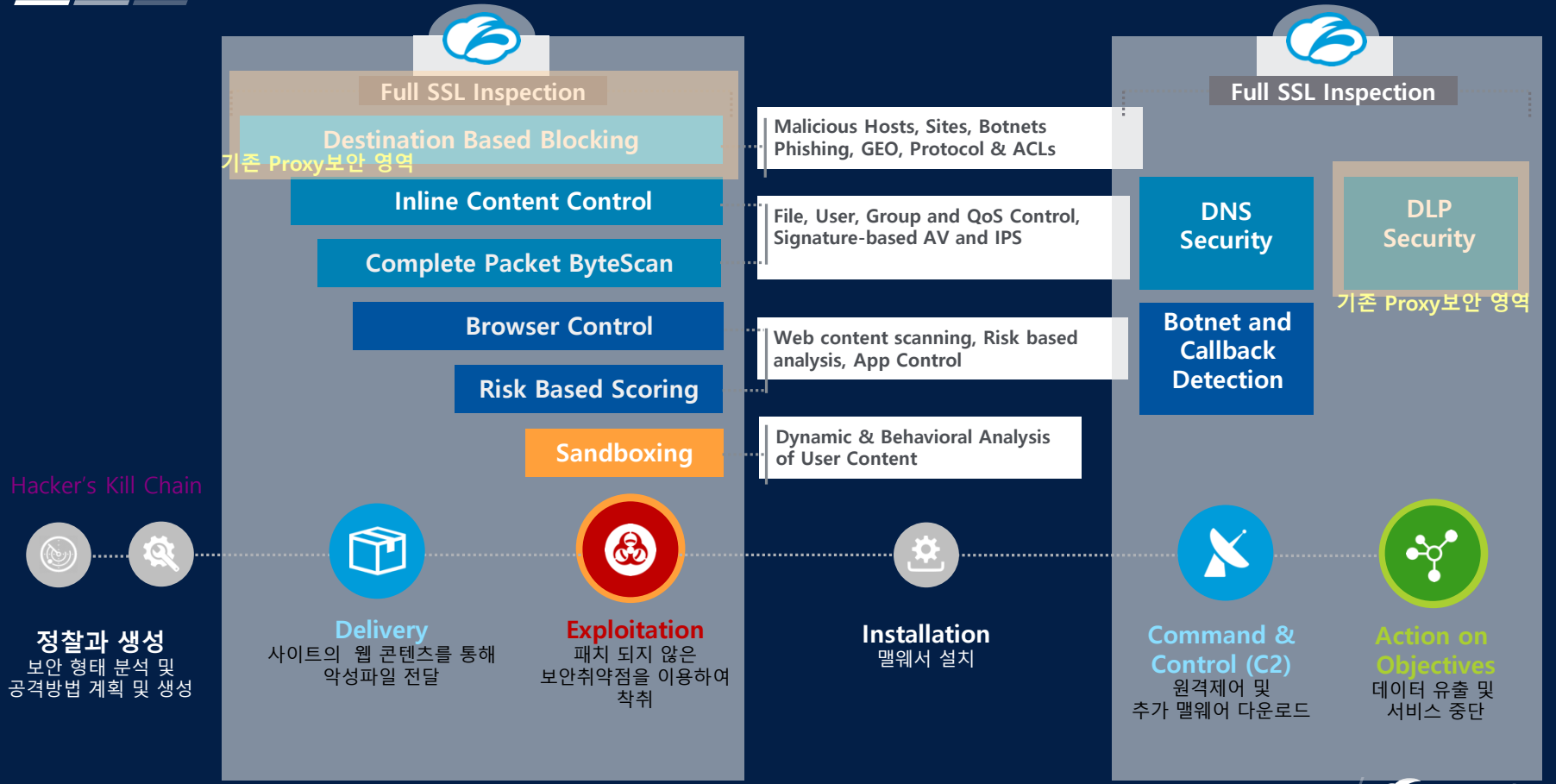
**125 Million** ← Find once, block everywhere
**Threats blocked per Day**



Securing your cloud transformation

zscaler™

# Zscaler Hacker의 Kill Chain 파괴 기능

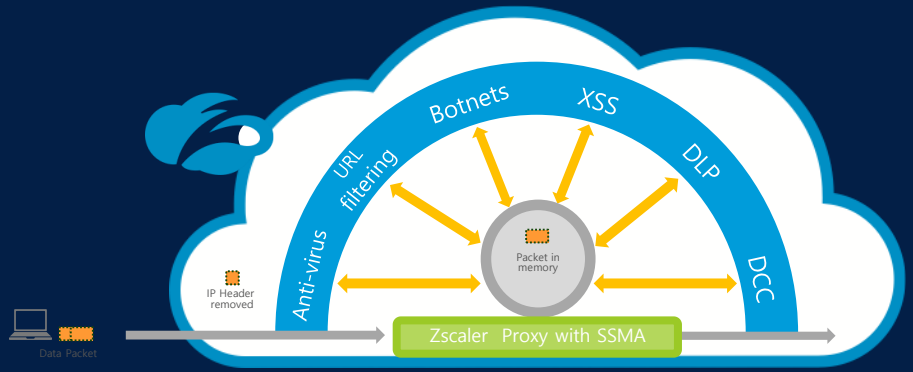


# 보안 관리에 대한 일관성 있는 기준과 관리 부재 해결

| On-Premise Stack | Zscaler Stack |
| --- | --- |
| ✗ 복잡한 HW & SW의 라이프사이클에 따른 재배치 필요 | No Hardware / No Software의 OPEX 모델 ✓ |
| ✗ 사용자 보안은 On-Premise가 설치된 위치에서만 적용 | Any Where, Any Device 사용자 단말 보안 ✓ |
| ✗ 복잡한 보안장비의 로그 통합 수집 및 가공의 어려움 | 통합된 전체 로그 분석 - Zscaler Portal ✓ |
| ✗ 제한적인 SSL 적용으로 인한 높은 보안 부재 발생 | 모든 보안 기능에 Full-Inline SSL 적용 ✓ |
| ✗ 다양한 보안 기능의 완벽한 통합 불가능 | 단일 벤더의 완벽한 보안기능 통합 ✓ |
| ✗ 복잡한 보안장비로 인한 사용자 체감 속도 저하 | 고성능 ZEN노드를 통한 사용자 체감 속도 향상 ✓ |
| ✗ ID기반과 IP기반의 혼재된 보안 감사 | ID/IP기반의 통일된 보안 감사 가능 (User – APP) ✓ |
| ✗ 사이트 별 일관성 있는 보안 기능과 정책관리 부재 | 글로벌 보안 정책의 일관되고 지속적인 보안 정책 적용 ✓ |

# Ultra Low Latency 구현 : Zscaler의 특허기술

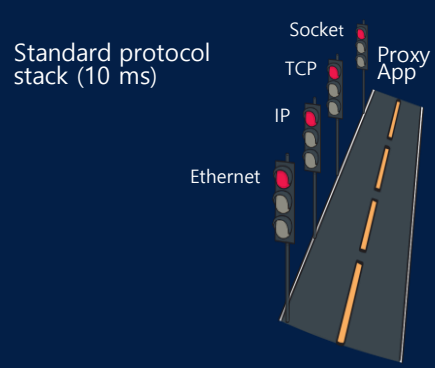
## SSMA(Single Scan Multi Action) 특허기술

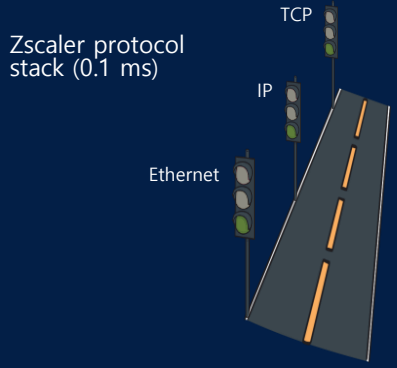



- **ZEN (Zscaler Enforcement Node)의 특성**
  1. One Vendor 솔루션
  2. One UI (중앙집중식 통합관리)
  3. One Action (동시 처리, Sandbox기능은 RAM DISK 기술을 통해 처리)
  4. ZERO Copies (고객의 트래픽 저장 없음)

- **낮은 Latency기술을 통해 할 수 있는 서비스**
  1. 고객의 가입서비스와 상관없이 항상 모든 보안기능에 대한 트래픽 검사 가능
  2. 동시 처리기술에 의해 모든 보안기능을 적용하여도 추가 성능저하 없음
  3. 고객은 필요한 추가적인 보안기능이 무엇인지 알 수 있도록 제시 가능

## TCP Stack 특허기술




패킷은 각 프로토콜 교차점에서 중지되고 큐잉되며 이로 인해 다음을 야기시킴:

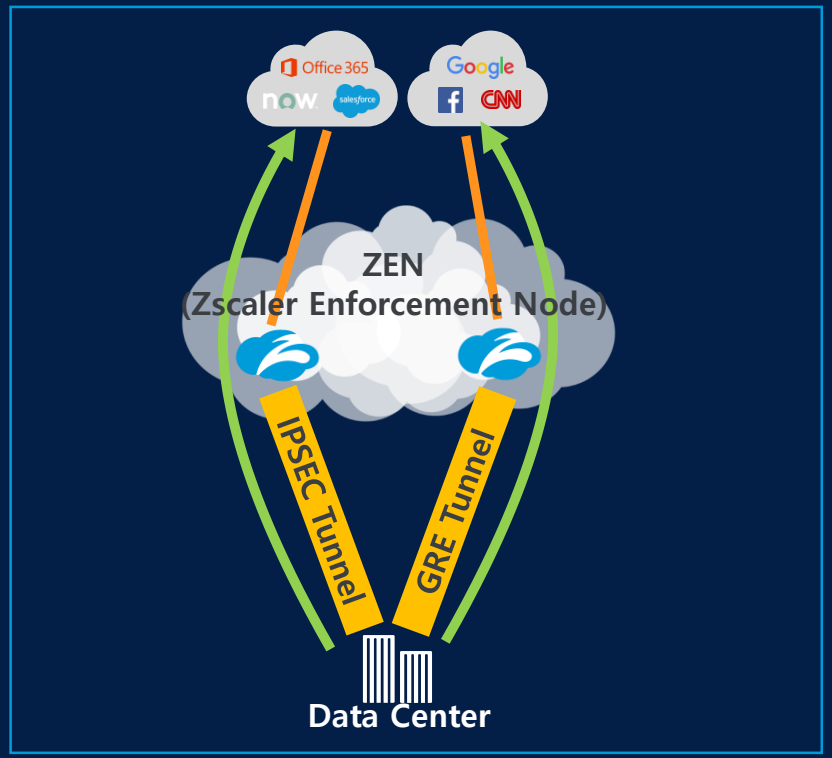
- Context switches
- Cache thrashing
- Memory waste

최적화된 TCP Stack 구현을 통해 :

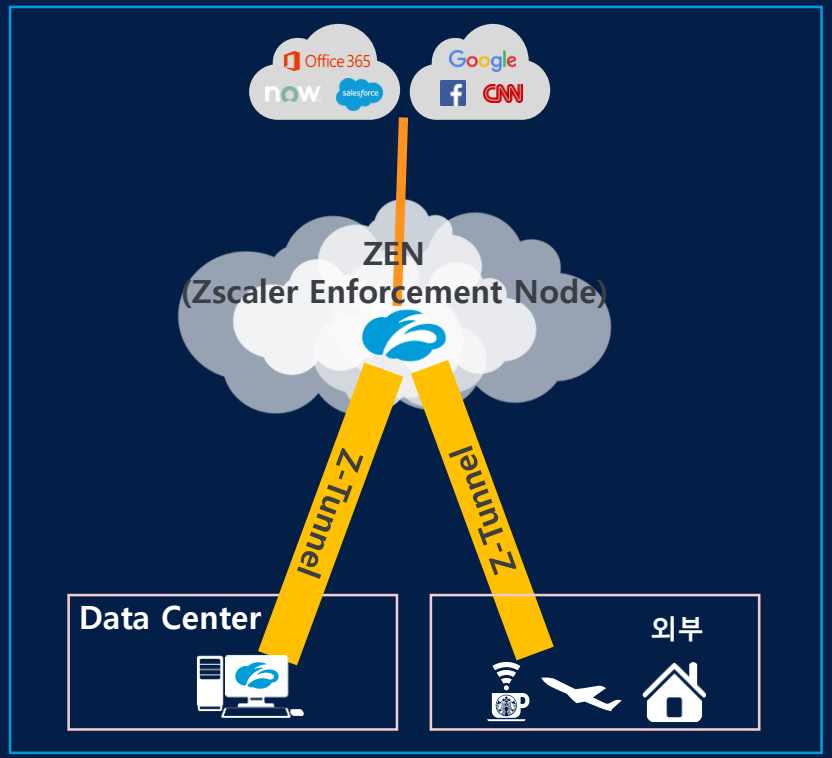
- 모든 중지와 큐잉 제거
- No context switches, Speed Connection
- 불필요한 구조인 소켓 제거
- Zero copy

# Zscaler Internet Access 구성 방식

## Tunnel 방식 (GRE or IPSEC)

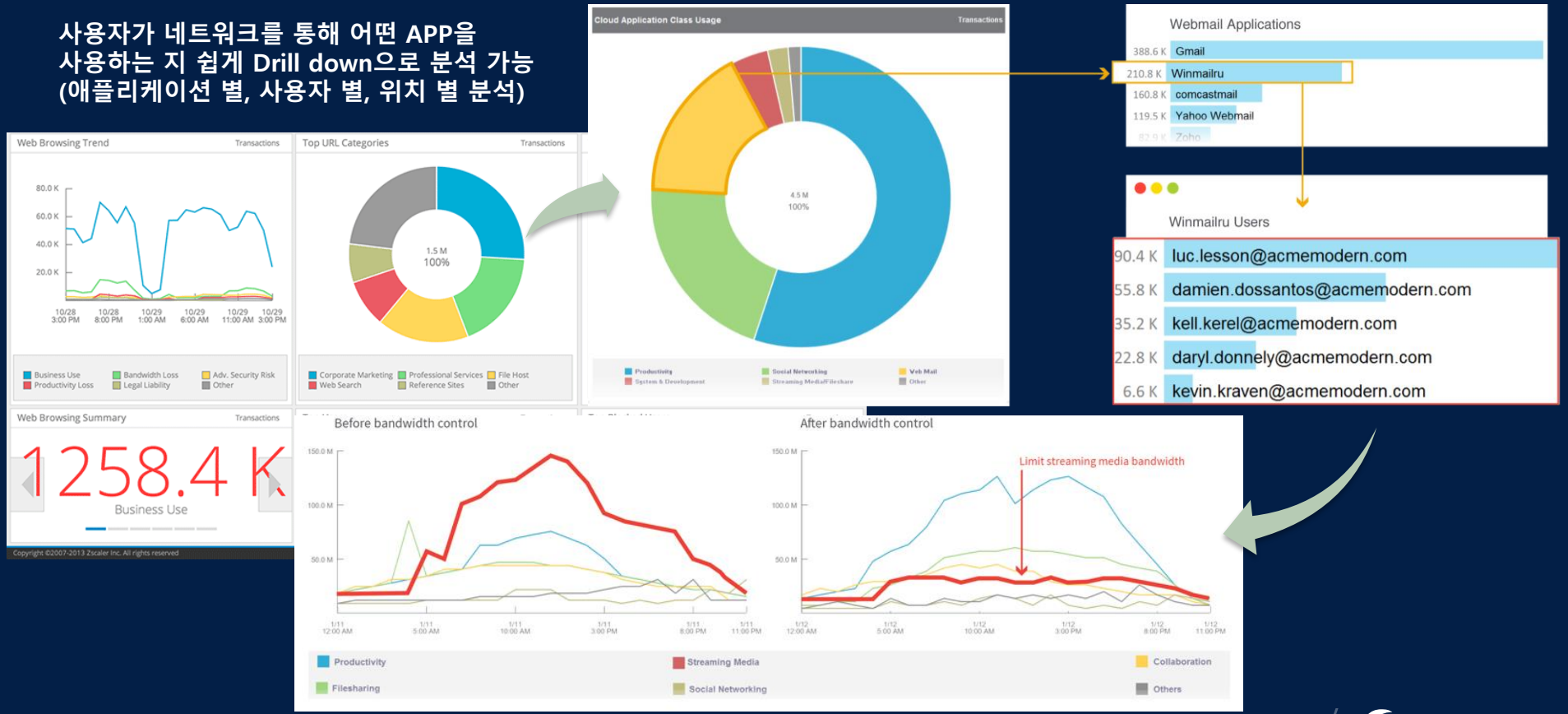



## Agent 방식 (Z-Tunnel)



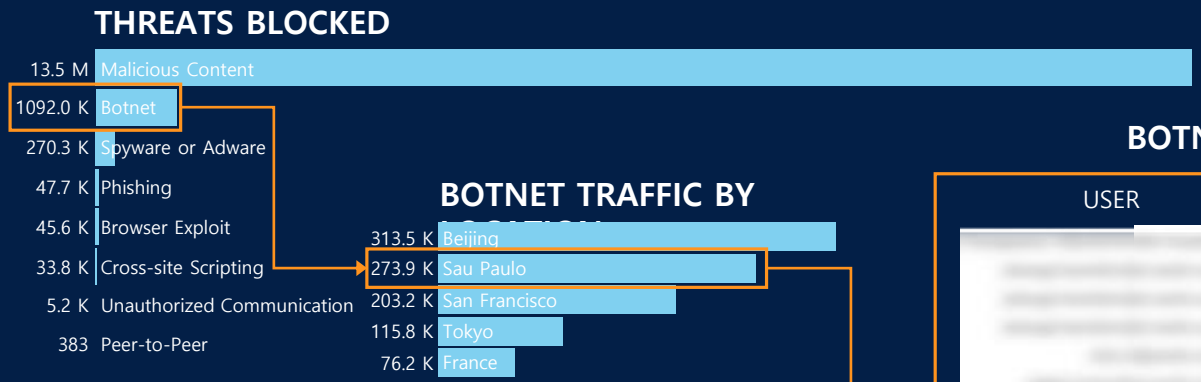
# Zscaler Internet Access UI

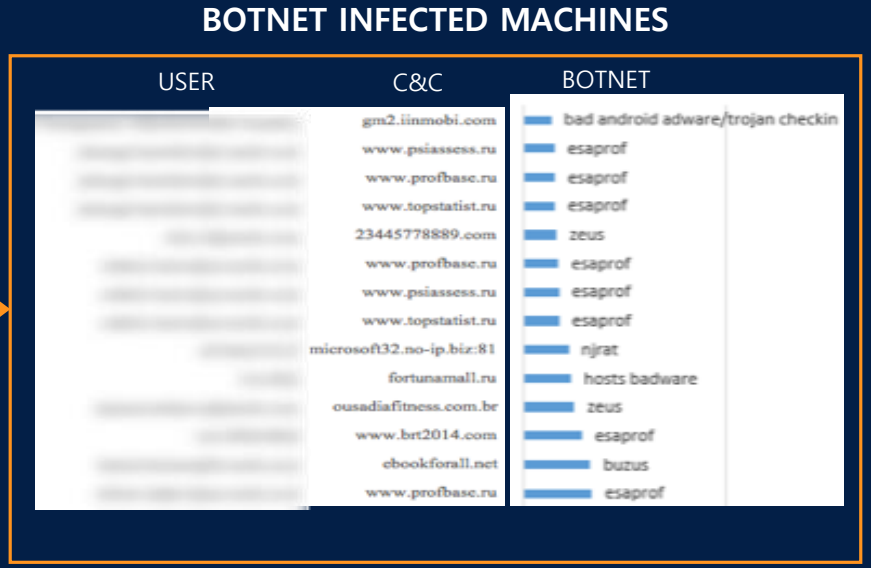
사용자가 네트워크를 통해 어떤 APP을
사용하는 지 쉽게 Drill down으로 분석 가능
(애플리케이션 별, 사용자 별, 위치 별 분석)



# 직관적인 전세계 사이트 관제 및 감염 단말 검출

**전세계의 해외 사이트에 대한 관제 및 감염 단말의 손쉬운 Drill Down 화면 제공**




예)
- Beam Suntory : 직원 150,000명, 3개월간의 데이터 검색
- 1,300만 건의 감염 사이트 접속 시도 및 차단
- 100만 건의 Botnet 사이트 접속 시도 및 차단
- 감염 내용→발생 위치 파악→해당 감염단말 파악→단말 조치

# ZPA(Zscaler Private Access)

# ZPA를 활용한 Zero Trust Network Access


## 사용 사례

### Remote Access VPN 대체

- 빠른 직접 연결
- 안전한 외부작업자들의 데이터센터 접속

### 멀티 클라우드에 직접 연결

- 데이터센터와 클라우드의 직접 연결이 불필요
- Virtual DMZs 제거

### M&A에 의한 IT 통합을 신속하게

- 네트워크 통합과 상관없이 업무 통합 가능
- 표준화된 보안정책 즉시 배포

### Secure Access to Industrial Systems

- Secure critical infrastructure (invisible)
- 정책 기반의 접속 허용, anywhere

**Zero Attack Surface • App Segmentation • Zero Trust Network Access**

## 플랫폼 서비스

### Zero Trust Network Access

Anti-VPN
Anti-Firewall
Anti-DDoS
Anti-Network Segmentation

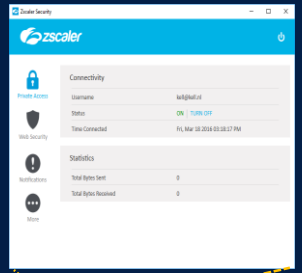
### Discovery/ Availability

GSLB
Optimal Path Selection
App Health Monitoring
App Discovery

### App/Device Access

Browser Access
Web Isolation
Private Service Edge

# ZPA를 활용한 Zero Trust Network Access



**임직원**
Intranet 및 데이터센터 모든 애플리케이션 이용

원격사용자
(Zscaler App 설치)

**파트너**
데이터 센터 내 특정 애플리케이션만 이용 허가

파트너

Google Cloud Platform

amazon web services

ZEN
Connector

Intranet

Microsoft Azure

ZEN
(Zscaler Enforcement node)

POLICY

Central Authority

ZEN
Connector

File shares

Intranet

NETFacilities

Exchange

ORACLE

**Zscaler App** – 사용자에게 웹 보안 및 보안 원격접속 제공

**ZEN Connector** – ZEN과 애플리케이션의 연결 중계

**ZEN (Zscaler Enforcement node)** – 사용자의 해당 애플리케이션을 연결

**Central Authority** – 모든 정책을 관리

# ZDX(Zscaler Digital Experience)

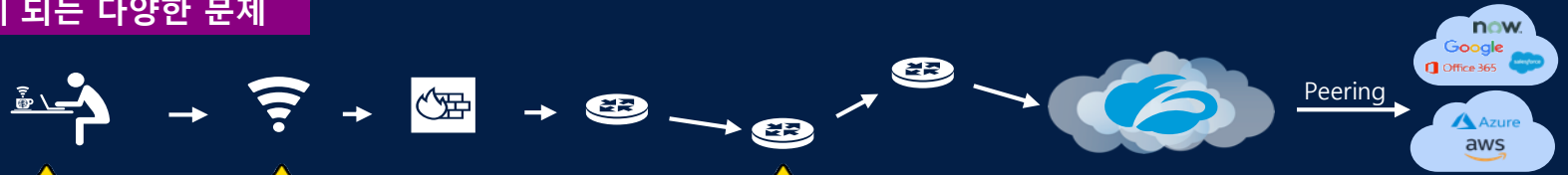
# 네트워크 모니터링의 한계

## 더 나아진 환경: 쉬운 설치 배포와 운영

**사내 접속 환경**


사내 Wi-Fi

**종종 겪게 되는 다양한 문제**




오피스365
업데이트 오류

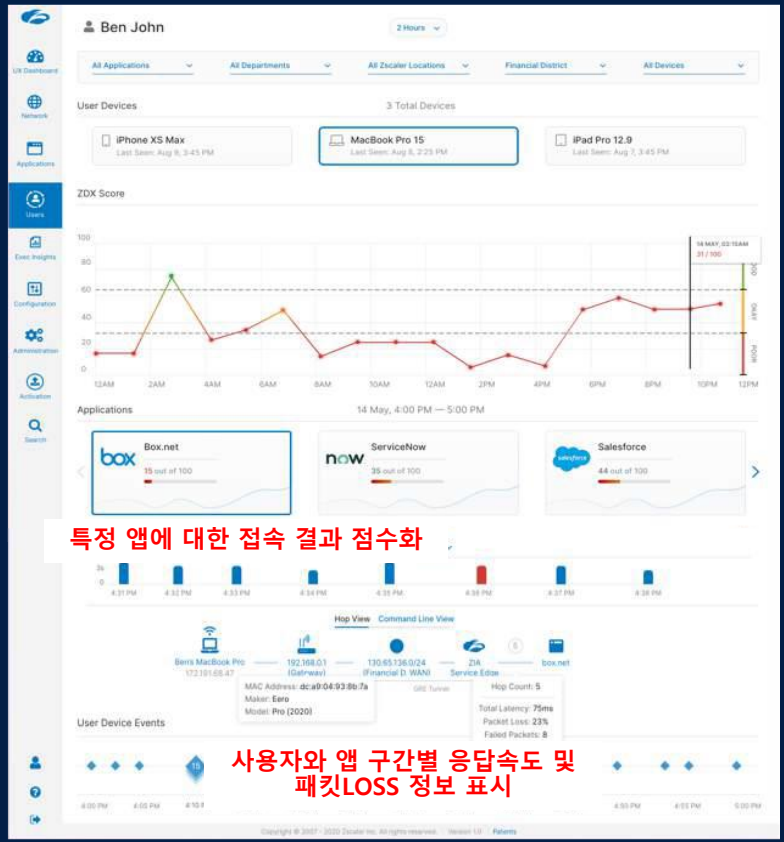
Wi-Fi
문제 발생

관리 범위를 넘어서는
인터넷의 문제

**인터넷 구간에 대한 가시성 확인의 어려움**

# ZDX - Zscaler Digital Experience

## 실시간 사용자 경험 및 서비스의 모니터링

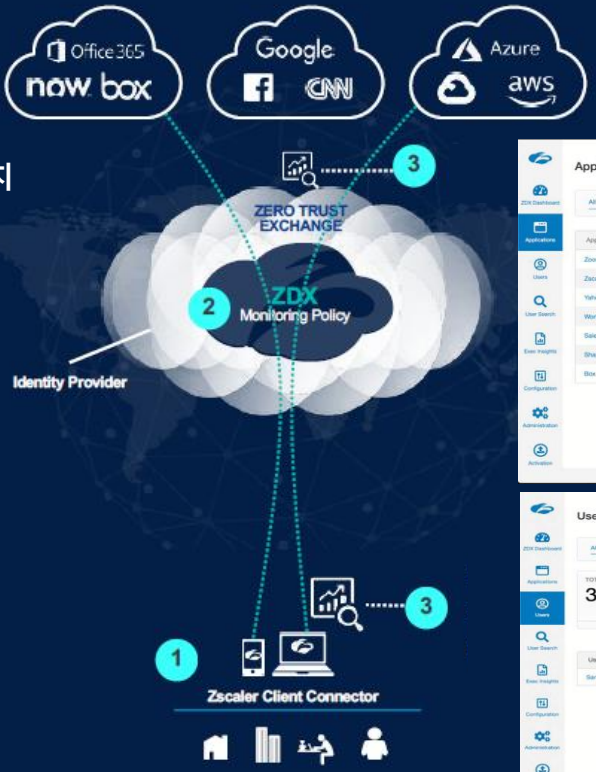



# 사용자 경험의 상시 모니터링

## 쉬운 설치 및 설정, 그럼에도 강력한 성능

### ZDX의 동작 원리

1. ZDX 기능이 설정된 에이전트 설치
2. 모니터링 정책 설정 및 적용
3. 설정 정책에 따른 상시 모니터링



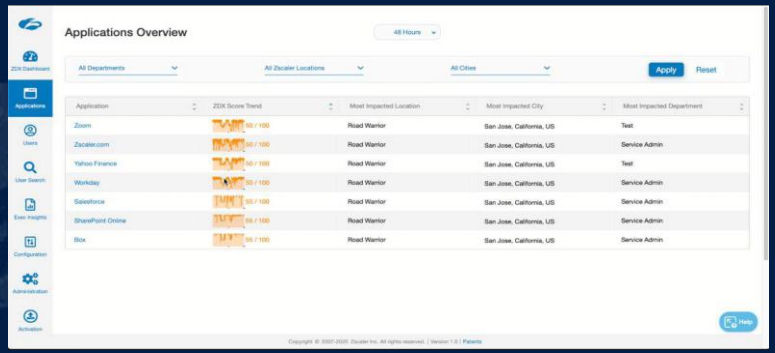

### ZDX의 사용 방법

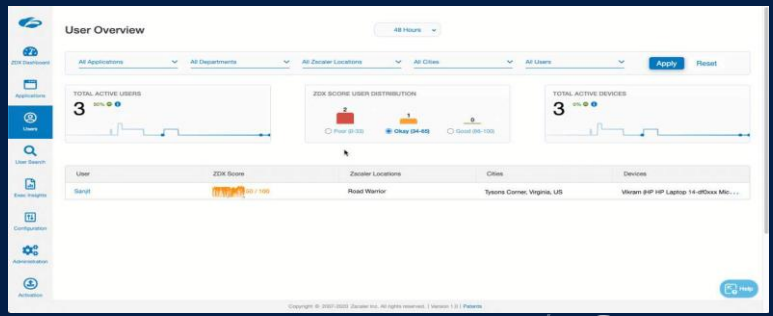
**End to End 가시성**

SaaS / 웹 애플리케이션 모니터링

**사용자 문제 확인 및 조치**

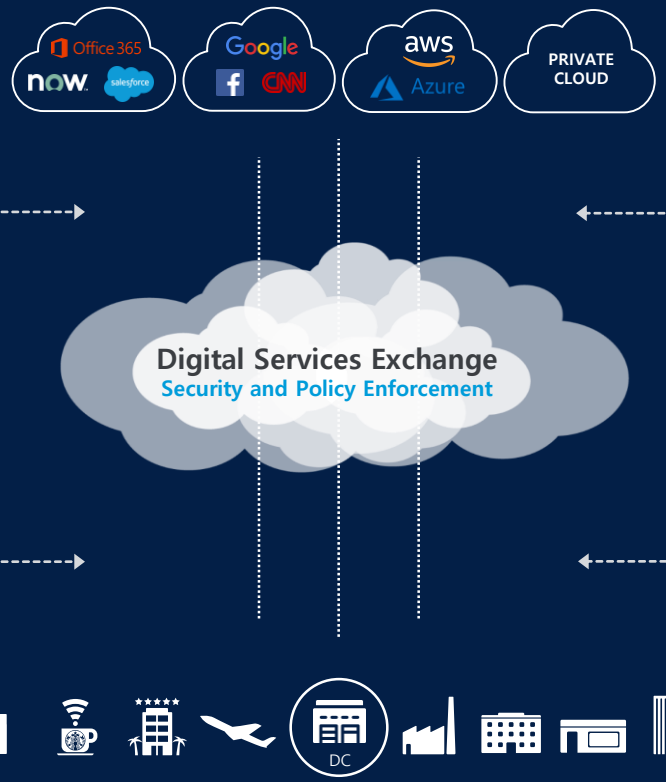
사용자 단말의 성능



# 클라우드 환경의 Partner ECO system

## 더 나아진 환경: 쉬운 설치 배포와 운영



# 3단계로 시작하는 Secure IT transformation 예제

MARS
100,000 Users / 85 Countries

UNITED
80,000 Users / 48 Countries

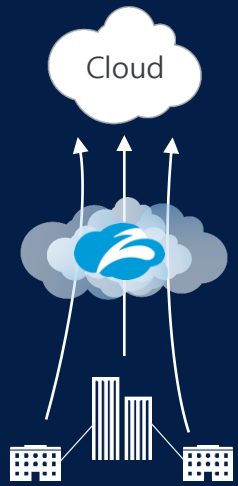
## SECURE
Up-level security


기존 인프라 변화 없이 모든 인터넷 트래픽을 Zscaler로 연결

## SIMPLIFY
Remove multiple point products


기존 보안 장비 추가 투자 감소, 보안 관련 복잡성 감소, 전용선 비용 감소

## TRANSFORM
Direct-to-cloud architecture




모든 사용자 인터넷 직접 연결
사용자 환경 개선, SD-WAN,
전용선 및 유지 관리 비용 감소

# Zscaler 도입 관점

## 위협 감소
## CISO

- 최상의 보안 상태 유지 비용
- 일관성 있는 보안 수준 유지 비용
- Any Where, Any Device 보안 비용

## IT 단순화
## CTO / IT Head

- 통합되고 심플한 IT구조
- 효과적인 클라우드 앱 사용과 관리 운영 비용
- 빠르고 쉬운 설치

## 인상적인 가치
## CIO / CFO

- 장비 투자 없는 탄력적인 비용구조
- 효율적인 관리 운영비용 절감
- MPLS 회선 비용 절감

## 생산성 향상
## End-users

- 사용자 체감 속도 향상
- 비즈니스 앱의 속도 보장
- 클라우드 앱 활용 증진

# 4가지 영역에서의 Zscaler 가치

### 기업의 경쟁력 강화

클라우드 도입의 촉매제

기존 네트워크와
보안의 한계 극복

### 증가하는 디지털화
### 자원의 보호

장소의 한계를 극복한
정책 기반의 액세스 제공

용량 한계를 극복한
Encrypted traffic 검사

### 고객과 사용자에게
### 향상된 사용자 경험 제공

앱과 사용자의 빠른 직접 연결,
블랙홀 제거

150 데이터센터를 통한 보안
정책과 실행 (SASE)

### 비용 절감과
### 미래 투자 보호

100% 클라우드 서비스 –
사용자 별

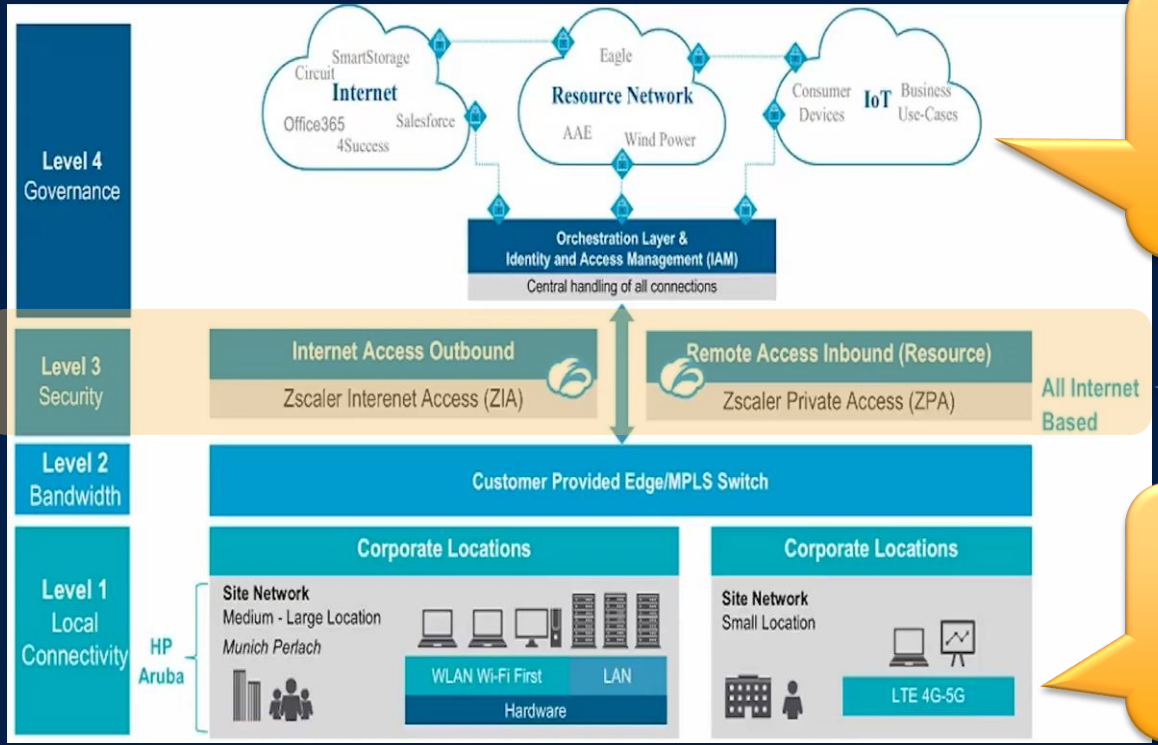
IT를 통합하고 복잡성 제거

"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.

# 업무환경 변화에 따른 Zscaler 구축 사례

- ✓ 해외 Siemens : 차세대 네트워크 보안
- ✓ Nov : ZeroTrust 보안 서비스 구축
- ✓ 그 외 국내 고객 사례

# SIEMENS의 차세대 네트워크와 보안의 핵심




**자원 네트워크의 목표**
- ✓ 모든 공격 및 악의적인 행동으로부터 자원 보호
- ✓ 기본 전송 계층은 인터넷으로 함
- ✓ 사용자와 장치에 대한 인증 체계 수립 (차등, 인증, 강도 사용)
- ✓ Micro Segment 화된 자원과 정책기반의 접속 제어
- ✓ 데이터 센터간 트래픽 최적화 (예. Public Cloud → Private Cloud)

**Zscaler 효과**
- ✓ 사용자 체감 속도 향상
- ✓ 비즈니스 리스크 감소 및 준수
- ✓ IT 간소화
- ✓ ROI 향상 및 비용 절감

**오피스 네트워크의 목표**
- ✓ 기업의 네트워크는 인터넷
- ✓ 클라우드로 원활하고 빠르게 접속하도록 함
- ✓ Wireless 우선 및 LAN 최소화
- ✓ MPLS보다 Local Internet 접속의 우선순위 높임
- ✓ 맞춤형 성능 및 아키텍쳐 (예. 실시간 프로토콜)
- ✓ 다층 보안으로 느려진 인터넷 성능을 직원의 집에서 경험하는 수준으로 높임

위치: 텍사스 주, 미국

업종 : 오일 & 가스

사용자 수 : 직원 64,000명

Zscaler 상품 : ZPA, ZIA

활용 사례 :
- Zero Trust 보안
- Third-party 위험 감소
- M&A 가속

## 도전

- 클라우드 환경 내에서 혁신적으로 보안을 수용할 수 있는 방법을 찾고 있었음
- 내부뿐만 아니라 네트워크 밖에 있을 때 수천 명의 사용자를 볼 수 있는 기능이 필요
- 지난 15년 이상 동안 300개 이상의 인수합병 활동이 있었음, IT가 활동을 통합할 수 있도록 하는 시간이 짧을 때 문제가 발생

## Zscaler 플랫폼의 이점

- ZPA와 Zero trust 전략을 채택할 수 있었음, 이제 해커들은 보이지 않는 것을 공격할 수 없음
- ZPA 커넥터에 의해 발견되고 있는 7,500개의 앱 중 3,400개는 원격 사용자가 액세스
- 단일 보안 플랫폼을 구축. ZIA와 ZPA로 인터넷 접속을 확보하여 내부 앱에 안전하게 접속
- WAF, DDoS 및 기타 구성 요소에 대한 비용을 절감
- 브라우저 액세스 기능 활용
- 빠른 ZPA 구축은 M&A의 시간을 단축하는 동시에 보안을 보장

# Zscaler 도입 목적 및 효과

| | |
|---|---|
| 비즈니스 리스크 감소 | • 표준화된 전사적 보안 정책 수립 및 실행<br>• 실시간 최신 보안 서비스를 통한 탁월한 위협 탐지<br>• 이동 사용자 영역까지 보안 정책 확대<br>• 모든 사용자에게 동일한 보안 서비스 제공 |
| 비용 절감 | • 전용선 유지 비용 감소<br>• 불필요한 고비용의 장비 구매, 설치, 유지 보수 및 교체<br>• 전용선을 통하지 않고도 보안 정책이 적용<br>• 트래픽 증가로 인한 전용선 서비스 지연과 혼잡 제거<br>• 중복된 기능의 투자 방지 |
| 생산성 향상 | • 업무용 트래픽에 우선 순위 부여, Bandwidth Control<br>• 기존 네트워크 설비의 생산성 향상<br>• 보안 업데이트 및 패치 관리에서 해방<br>• 클라우드 플랫폼을 통한 실시간 자동 업데이트 |
| 관리 편의성 | • 다양한 정책으로 본사, 지사, 원격지, 협력사 통합 보안 서비스 제공<br>• 간편한 서비스 연결과 쉬운 장애 처리<br>• 손쉬운 기능 추가와 정책 설정 및 실행, 그룹별 관리<br>• 규모의 변화나 위치에 상관없이 일관적인 서비스 관리 |


영업 문의 biz@expernet.co.kr
기술 문의 sase@expernet.co.kr



Securing your cloud transformation

zscaler™