

ISEC 2024



Ready for anything

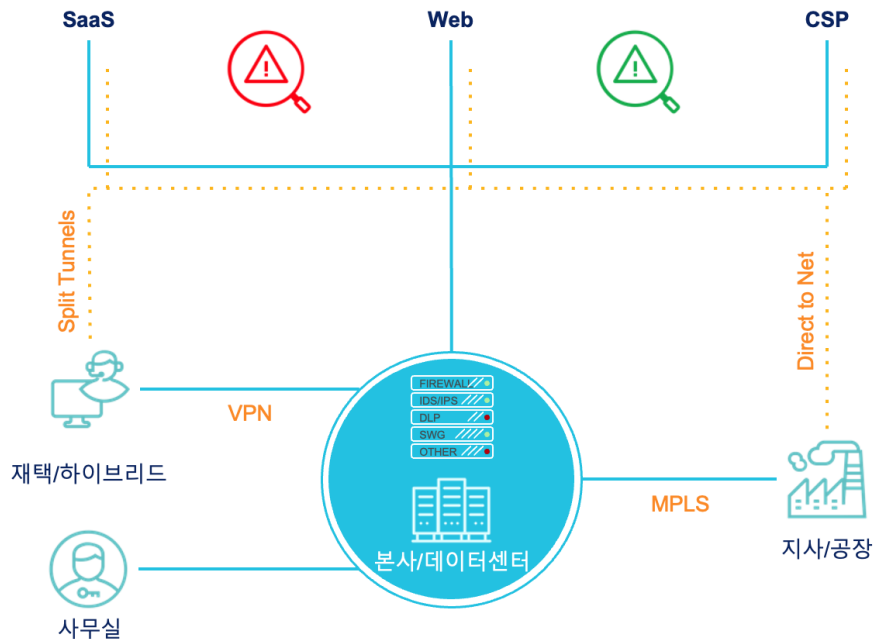




클라우드 시대의 정보 보안



기존 환경



1. 관문에 몰리는 트래픽의 부담

- . 비용
- . 네트워크 구성
- . 확장, 축소의 효율화

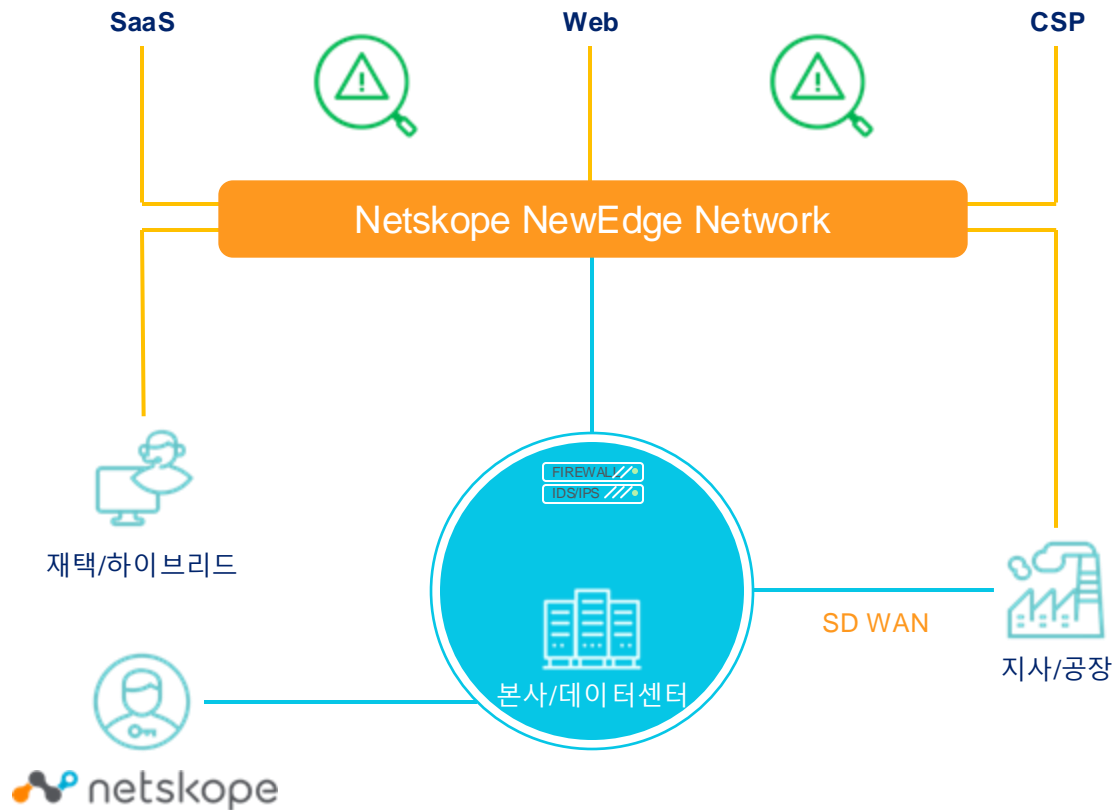
2. 인터넷 직접연결로 인한 감염 및 전파

- . Split Tunnels
- . Direct to Internet

3. 개인 사용자 및 지사에 대한 추가적인 보안 대책

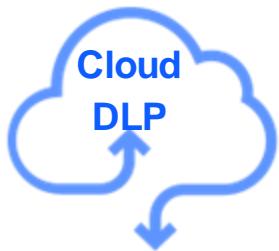
- . SSL + 보안

클라우드 시대의 보안



1. 클라우드 (인터넷) 앱으로의 정보 유출 방지
2. SaaS의 보안대책
3. 성능 및 확장성
4. 보안 강화
5. 일관된 보안 수준 및 관리

클라우드 시대의 정보 보안



1. 클라우드 (인터넷) 앱
으로의 정보 유출 방
지

클라우드 App
으로의 데이터
유출 방지



2. SaaS의 보안대책

SaaS App의
제어 및 데이터
보호



3. 성능 및 확장성
4. 보안 강화
5. 일관된 보안 수준 및 관리

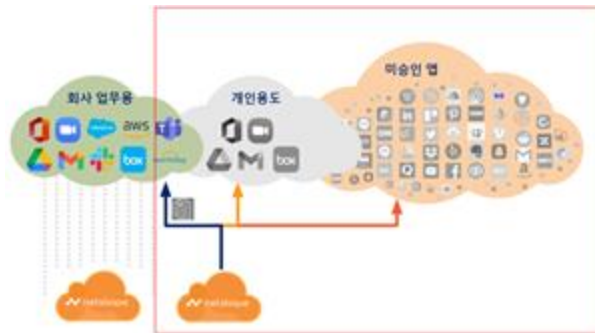
인터넷 트래픽
Threat Protection

클라우드 보안 - Cloud DLP

클라우드를 대비한 보안



클라우드 App
으로의 데이터
유출 방지



1. 클라우드 (인터넷) 앱으로의 정보 유출 방지

원천차단?

IT LED
5% apps
managed by IT

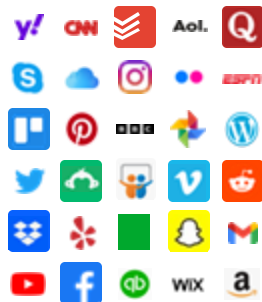
BUSINESS LED
95% apps
unmanaged

USER LED
Choice of
40,000+ apps

WEB
1.5 Billion
websites

2,400+
SaaS apps
per enterprise

95%
Shadow IT



원천차단?



[차단시]

- IT 헬프 데스크로의 문의 증가
- 사용자 불만 야기

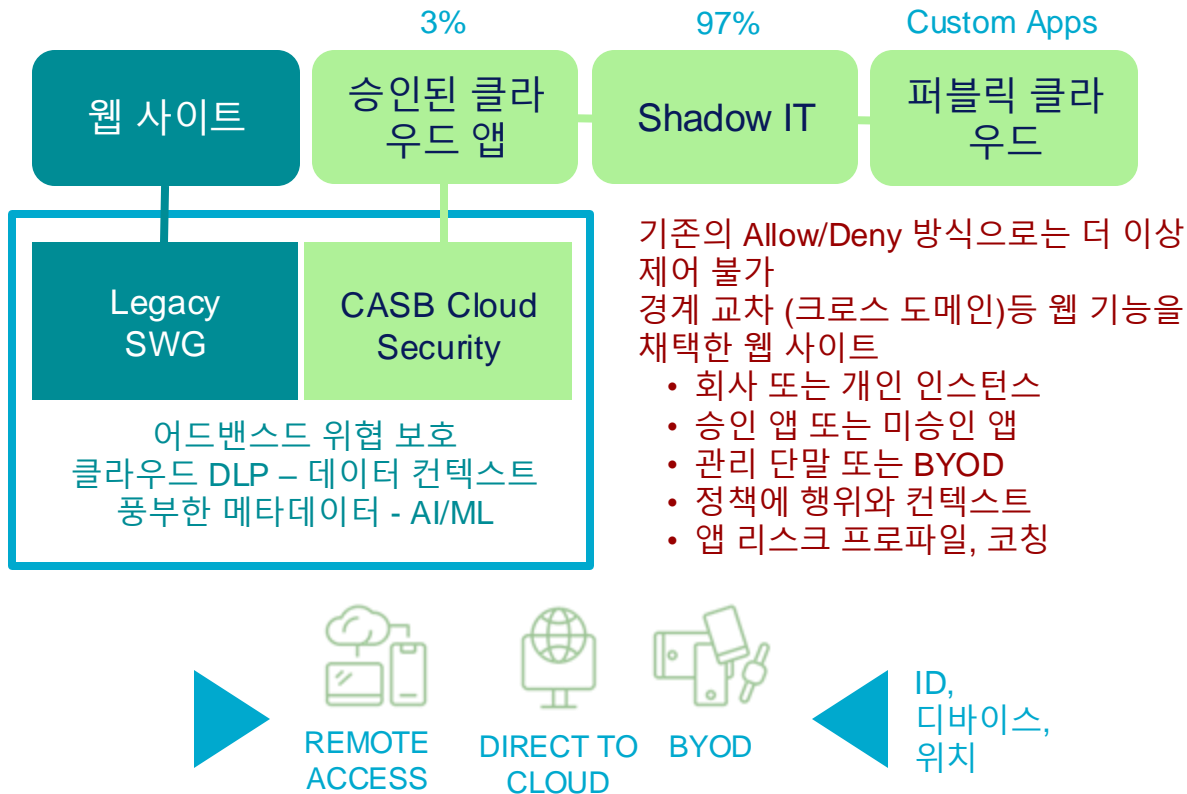
[허용시]

- 악성코드 감염 가능성
- 지속적 관리 및 모니터링

[한 줄 요약] 분류되지 않은 위험한 웹사이트를 격리하여 최종 사용자 기기에서 웹사이트 코드가 실행되지 않도록 보장 필요

원천차단?

- SaaS에 사용의 증가. SaaS의 경우 기존 SWG로는 제어 불가
- 코로나 이후로 재택 근무자 증가. 기존 온프레미 기반으로 통제 불가
- 68%의 위협이 클라우드를 통해 전파, 클라우드 트래픽이 웹보다 많음
- SaaS 가 #1 피싱 타겟
- 클라우드 스토리지가 위협의 소스로서 가장 많이 사용 (OneDrive, Box, G-Drive)



클라우드 데이터 유출



[사례]

- 위험을 인지하지 못하고 익숙한 도구로 생산성을 높이기 위해 승인되지 않은 도구에 접속

[사용자 코칭]

- 위험한 행동을 피하는 방법에 대한 명확한 적시(Just-In-Time) 피드백을 제공
- 동시에 목표를 달성할 수 있는 더 안전한 대안을 제시

사용자 보안 의식 향상을 위해 실시간 피드백을 제공하는 유연한 코칭 필요

CCI : Cloud Confidence Index

Cloud Confidence Index (CCI)

All Apps [RESET SCORES] [CANCEL] [APPLY CHANGES]

CCI LEVEL [30,357 matches found.]

Search App Name [Search for apps by name]

CUSTOM APP TAGS

All Custom Tags

APPLICATION CATEGORIES

All Categories

- Advocacy Groups & Trade Associations
- App Admin Console
- Application Suite

Application	CCI Score
SICLOPE erplan.com.br The SICLOPE is a cloud-based application. The solution was designed to guarantee information available, problem knowledg...	96
Amazon Database Amazon Database provides managed database services that includes relational databases for transactional applications, non...	96
Amazon Relational Database Service rds.us-east-1.amazonaws.com Amazon Relational Database Service (Amazon RDS) enable to set up and operate a relational database in the cloud. It assists in...	96
Amazon Web Services aws.amazon.com Amazon Web Services provides companies with an infrastructure web services platform in the cloud. Companies can requisite...	96
Google enote-rhrs	96
Microsoft Azure	96

CCI : Cloud Confidence Index

Cloud Security Alliance의 Cloud Controls Matrix 프레임워크 기반

CCI Score Range	Corresponding Cloud Confidence Level		Example from the CCI
90-100		Excellent	 
75-89		High	 
60-74		Medium	 
50-59		Low	 
0-49		Poor	 
N/A		Under Research	 
Pending Change		Pending Changes	  → 

- 컴플라이언스 인증, 데이터 센터 표준
- 데이터 암호화, 테넌트 분리, 취약한 Cipher Suite
- SSO/SAML, IP 주소 기반 제한, 역할 기반 권한 부여
- 관리자 및 사용자 감사 로그, 데이터 접근 감사 로그
- 재해 복구 및 비즈니스 연속성: 인프라 상태 보고서, 업그레이드 및 유지 관리
- 법률 및 데이터 소유권
- 침해 여부, 보고된 취약점

클라우드 보안 - SaaS Apps

클라우드를 위한 보안



2. SaaS의 보안대책



SaaS App의
제어 및 데이터
보호

가시성 결여

	애플리케이션	분류	총 다운로드	총 업로드	# 사용자	# 세션
1	Google Chat	협업	53MB	54MB	2	14
2	AWS Console	IaaS/PaaS	43MB	33MB	1	12
3	Slack	협업	40MB	11MB	3	9
4	Google Drive	클라우드 스토리지	35MB	10MB	1	7
5	Naver	검색 엔진	30MB	3MB	1	7

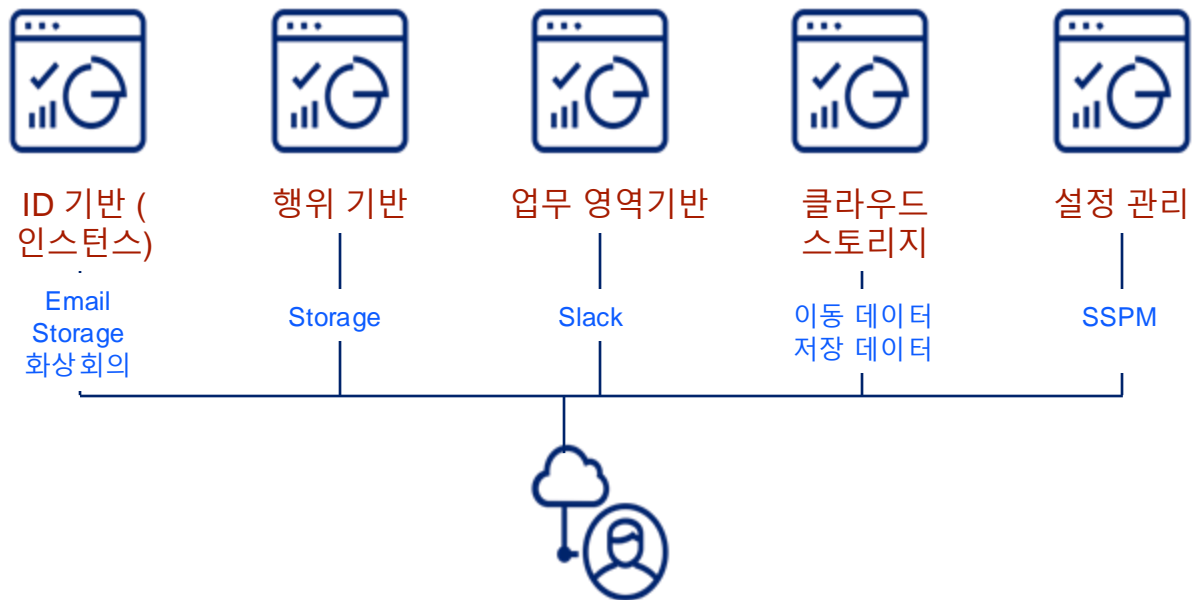


[가시성 결여]

- 앱 정보: 위험도, 인가 여부, 시간대별 사용량
- 주요 활동: 생성, 편집, 초대, 공유, 로그인, 다운로드
- 접근 위치: 한국, 해외
- 인시던트: DLP, 멀웨어

인가된 혹은 인가되지 않은 앱을 통해 발생하는 모든 활동에 대한 가시성 확보가 필요

SaaS 보안 요소 - 가시성 확보 요소



전체 컨텍스트를 파악하여 제로 트러스트를 구현

사용자
신뢰

디바이스
신뢰

로케이션
신뢰

앱 안전도
신뢰









앱 인가
신뢰

인스턴스
신뢰

행위
신뢰

데이터
신뢰

허용
차단
코칭
인증
판단
격리

Identity	Device Risk	SaaS App	App Instance	App Risk	URL Category	Activity Controls	User Risk	Threat	Data Risk (DLP)	Policy Action
 Pat Smith Accounting Logged in as psmith@ gmail.com	 Unmanaged  Personal/ BYOD	 Google Drive Sanctioned Unsanctioned	 Company  Personal	 93 Excellent rating (low risk) Breadth of 80K+ Apps	 Cloud Storage 130+ categories	 Upload Share Create Delete Move Download (120+)	 863 Behavior Tracking (moderate risk) (UEBA)	 Threat Intel AV Sandbox IPS ML CTE	 GDPR AU Privacy Act Over 3000+ classifiers	 Contextual: Allow Coach Block Encrypt Legal Hold Quarantine MFA

클라우드 보안 - 효율성 및 확장성

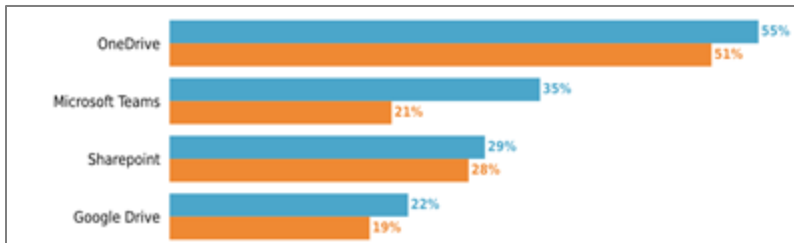
- 3. 성능 및 확장성
- 4. 보안 강화
- 5. 일관된 보안 수준 및 관리

클라우드를
이용한 보안



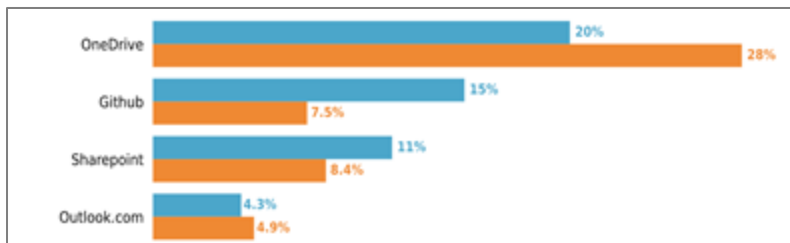
인터넷 트래픽
Threat Protection

SSL traffic



인기있는 클라우드 앱

- 금융 서비스 부문의 사용자는 한달에 평균 23개의 클라우드 앱과 상호 작용
- 금융 서비스의 경우 Teams 사용률이 높음



악용되는 클라우드 앱

- 다른 산업에 비해 OneDrive에서의 멀웨어 다운로드가 적음
- SharePoint에서의 멀웨어 다운로드는 Teams의 인기와 관련 있을 가능성이 높음
- 대다수의 공격자는 SharePoint를 사용하는 Teams에서 파일 공유를 통해 멀웨어 전달을 시도

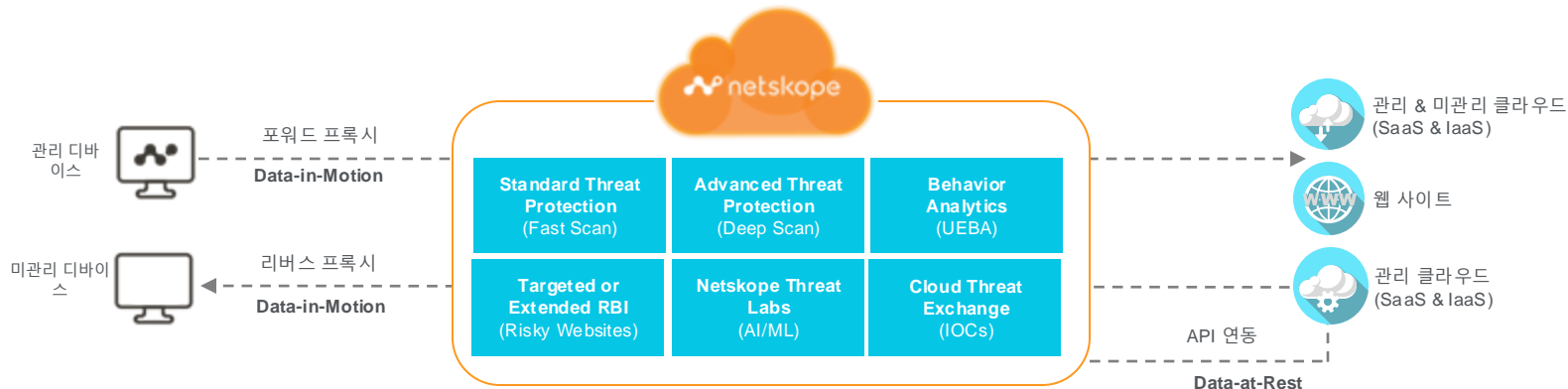


[성능 vs 보안]

- **MS 권장:** 트래픽에 대한 암호 해독 및 애플리케이션 프로토콜에 대한 특정 작업 수행 시 성능 저하를 경험할 수 있음
- **성능 고려사항:** 복호화를 수행하는 장비의 용량, 트래픽 지연
- **보안 고려사항:** 실시간(+주기적) 탐지 및 제어, 동적 분석 지원

[한 줄 요약] 모든 웹 및 클라우드 트래픽의 HTTP 및 HTTPS 다운로드를 검사하여 멀웨어의 침투 방지 필요

최신의 위협에 대비할 수 있는 심층 분석



Fast Scan

- 멀웨어 방지 엔진, 웹 IPS, 실제 파일 유형 분석 및 ML 기반 피싱 탐지
- 40개 이상의 위험 인텔리전스 피드 및 악성 URL 및 파일 해시를 포함한 IOC 가져오기
- 알려지지 않은 멀웨어 탐지 및 차단을 위한 인라인 실행 파일(PE) 파일 머신 러닝
- 모든 AV/ML 탐지를 위한 파일 샌드박스
- 위험 인텔리전스의 양방향 IOC 공유를 위한 클라우드 위협 교환(CTE)

Deep Scan

- 350개 이상의 설치 프로그램, 패커, 압축기 제품군을 지원하는 난독화 해제 및 재귀적 파일 언패킹
- 3,500개 이상의 파일 형식 계열에 대한 사전 실행 분석 및 휴리스틱과 3,000개 이상의 정적 바이너리 위험 지표를 지원
- 동적 파일 분석을 통해 30개 이상의 파일 유형에 대한 클라우드 샌드박스 및 회피 기술 차단
- 알려지지 않은 위험, 이상 징후 및 행동을 탐지하는 머신 러닝 심층 분석
- 웹 브라우저 격리(RBI), 클라우드 방화벽

Behavior Analytics

- 대량 업로드, 다운로드, 삭제는 물론 근접성, 로그인 실패, 공유 자격 증명, 희귀 이벤트, 위험 국가, 회사 및 개인 인스턴스 간 데이터 유출(인라인 및 API)을 탐지하는 순차적 이상 행동 규칙
- 사전 정의된 템플릿을 사용한 사용자 지정 순차적 이상 징후 규칙
- 악의적인 내부자, 손상된 계정, 데이터 유출에 대한 머신 러닝(ML) 기반 이상 징후 탐지, 130개 이상의 탐지기와 65개 ML 모델을 사용한 사용자 신뢰 지수(UCI) 점수 산출

Cloud Exchange, 통합 그 이상의 가치

공격 대응력 향상



Cloud Log Shipper

- 자동화된 IOC 공유
- 양방향 업데이트
- 파일 해시, 악성 URL

신속한 사고 대응



Cloud Ticket Orchestrator

- 서비스 티켓 자동화
- 선별된 이벤트 세부 정보
- 워크플로우 연계

제로 트러스트 활성화



Cloud Threat Exchange

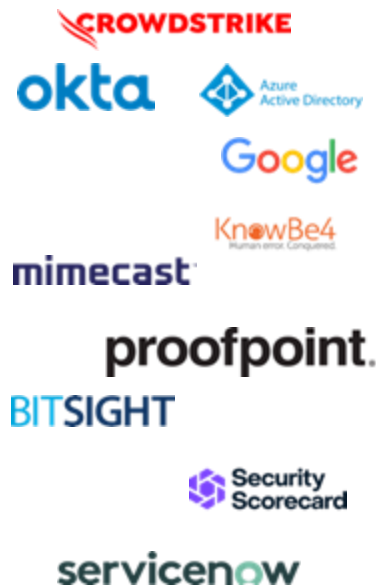
- 위험 점수 교환
- 사용자, 앱, 디바이스
- CTO 트리거

SOC 피드 및 XDR



Cloud Risk Exchange

- 이벤트/경고 추출
- 근실시간 수집
- N개의 목적지 설정





ZTNA

Zero Trust Network Access



netskope ZTNA

조직의 사내 애플리케이션을 제로 트러스트 방식으로 이용할 수 있는 클라우드 기반 서비스



- ✓ 사용자와 사내 앱은 서로 다른 최적의 NS-POP을 통해 연결
- ✓ 네트워크 경계가 아닌 클라우드에서 사용자 및 디바이스 인증
- ✓ 사용자, 디바이스별 접근 정책 및 권한 부여
- ✓ 종단간 통신 암호화
- ✓ 사용자를 네트워크가 아닌 승인된 사내 앱에 연결
- ✓ ZTNA 에이전트를 설치할 수 없는 환경을 고려한 브라우저 기반의 연결

ZTNA vs VPN



- 선 연결 후 인증
- 단순한 접근(All 또는 Nothing)
- 공격자에게 보이는 오픈된 포트
- IP 기반(디바이스를 네트워크에 연결)

VPN

ZTNA



- 선 인증 후 연결
- 세분화된 접근(측면 이동 제한)
- 외부에 노출되지 않는 자산
- 신원 기반(사용자를 특정 리소스에 연결)

기능	VPN	ZTNA
데이터센터(방화벽 하단) 리소스에 접근 가능	✓	✓
강력한 사용자 인증	✓	✓
디바이스 상태 확인	✓	✓
네트워크가 아닌 애플리케이션에 대한 액세스 제어	--	✓
다양한 클라우드 및 데이터센터 환경으로 확장	--	✓
사용자는 원격 접속에 대한 의식 불필요	--	✓
클라우드 서비스로 제공	--	✓



Netskope



- 설립: 2012년
- 본사: 미국 캘리포니아주 산타클라라
- 종업원 : 글로벌 3,000 명 이상
- 제삼자에 의한 평가 :
 - 🏆 2023 Gartner Security Service Edge(SSE) Magic Quadrant
→ 리더
 - 🏆 2024 Gartner Security Service Edge(SSE) Magic Quadrant
→ 리더



The Leading Secure Access Service Edge

- 파트너 기업과 강력한 기술 및 서비스 연계



- 실리콘 밸리 투자기업으로부터 1조4천억 조달



Gartner SSE MQ (3년 연속 TOP 리더)

Figure 1: Magic Quadrant for Security Service Edge



Source: Gartner

- SSE 부문 Gartner Magic Quadrant에서 3년 연속 리더로 선정
 - 가장 강력한 실행 능력과 가장 완전한 비전을 모두 갖춘 선두 자리를 유지
 - 3대 분석 회사 모두에서 SSE 시장의 리더로 인정
- Gartner: Magic Quadrant for Security Service Edge (April 2024)
 - IDC: Marketscape for NESaaS (June 2023)
 - Forrester: Wave for Security Service Edge Solutions (March 2024)

Netskope NewEdge Network

성능 저하없이 고도의 보안을 실현할 수 있는 글로벌 네트워크



80+
Regions



200+
Localization
Zones



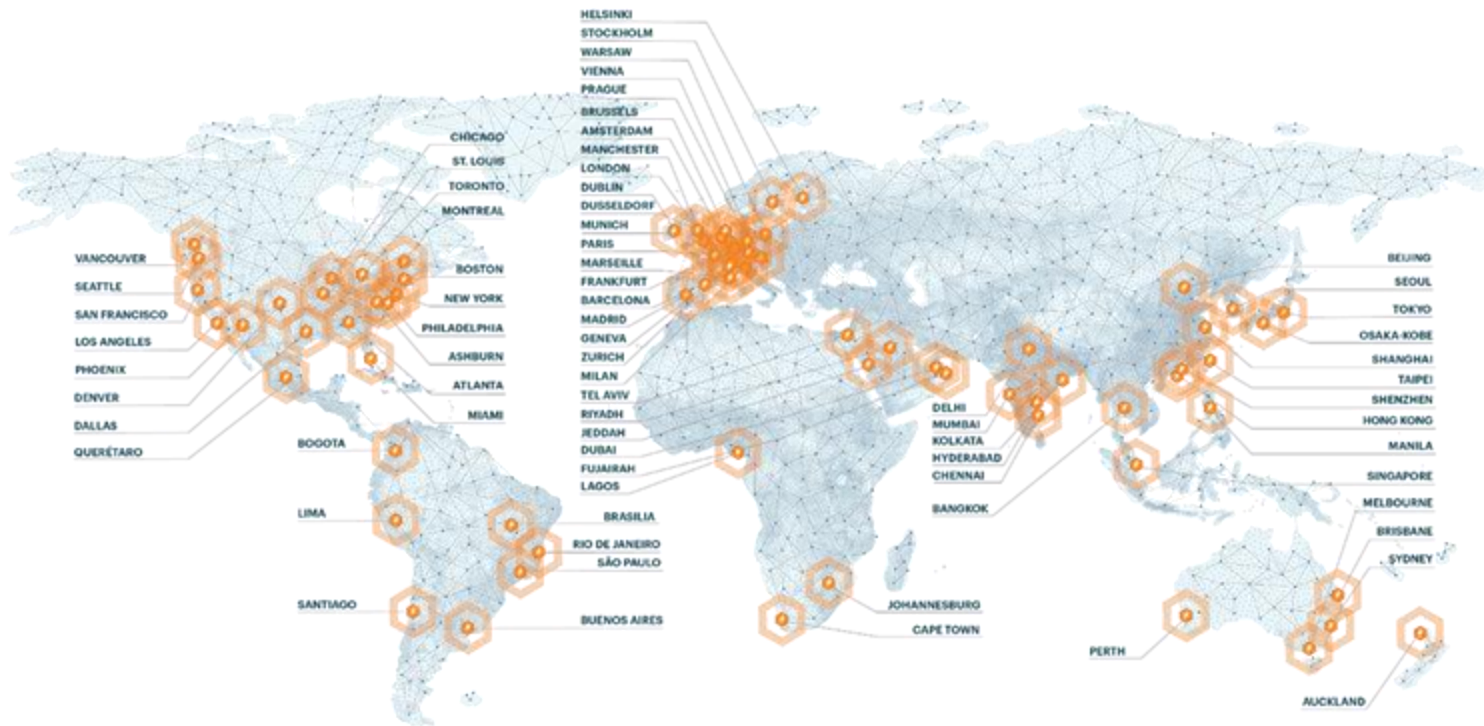
3K+
Network
Agencies



FULL
Compute



Industry's
Best
SLAs



Government
of Canada



International
Organization
for
Standardization



International
Electrotechnical
Commission



TRUSTe
Certified Privacy
Program



DATA PRIVACY
FRAMEWORK
PROGRAM



감사합니다