ZIA

Zscaler Internet Access™

AI 기술을 활용하여 모든 사용자, 앱, 위치를 보호하는 보안 플랫폼

zscaler™

Zscaler Internet Access

AI 기술을 활용하여 모든 사용자, 앱, 위치를 보호하는 보안 플랫폼

Zscaler Internet Access™는 업계에서 가장 포괄적인 제로 트러스트 플랫폼으로 안전하고 빠른 인터넷 및 SaaS 액세스를 제공합니다.

클라우드 서비스와 모바일 기기가 그 어느 때보다 중요해진 지금, 레거시 네트워크 보안은 그 효율성이 조금씩 떨어지는 양상을 보이고 있습니다.

레거시 허브-앤-스포크 형태의 아키텍처의 경우, 사용자는 주로 조직의 본사나 지사에, 애플리케이션은 조직의 데이터 센터에만 위치해 있고, 보안은 기업 내부의 한정된 영역에서만 효과를 발휘할 수 있었습니다.

그러나 오늘날 우리는 랜섬웨어, 암호화 기술을 이용한 공격, 공급망에 대한 공격, 기타 지능형 위협 등이 레거시 네트워크의 방어 체계를 충분히 무너뜨릴 수 있는 완전히 새로운 위협 환경과 세상에 살고 있습니다.

이에, 각종 기업은 사업 활동을 영위하는 데 도움이 되는 유연성을 갖추고 있으면서도 여러 위험과 복잡성을 전반적으로 줄여 주는 클라우드 네이티브 보안 솔루션을 찾아야 하는 시기에 직면해 있습니다.

Zscaler Internet Access

클라우드 및 모바일 플랫폼을 활용하는 기업의 경우 비지니스를 보호하기 위해서 제로 트러스트를 기반으로 하는 새로운 보안의 접근 방식이 필요합니다. Zscaler Zero Trust Exchange™ 솔루션에 포함되어 있는 Zscaler의 Zscaler Internet Access는, 지난 10년 간 보안 웹 게이트웨이 분야의 독보적인 리더로 평가 받고 있는 솔루션이며, 세계에서 가장 많이 배포된 보안 서비스 엣지(SSE) 플랫폼입니다. 세계 최대 보안 클라우드에서 확장 가능한 SaaS 플랫폼의 형태로 제공되는 해당 제품은 레거시 네트워크 보안 솔루션을 대체하여 지능형 공격을 차단하고 포괄적인 제로 트러스트 접근 방식으로 데이터 손실을 철저히 방지합니다.

특장점:

- **AI를 이용한 사이버 위협 대응 및 데이터 손실 방지:** 세계 최대 규모의 보안 클라우드를 이용하여 매일 300조 건의 위협 신호에 대한 정보를 실시간으로 업데이트하여 강화된 AI 기반 사이버 위협 및 데이터 보호 서비스 제품군을 통해 각종 지능형 위협으로부터 조직을 보호합니다.
- **타의 추종을 불허하는 사용자 경험:** 세계에서 가장 빠른 인터넷 및 SaaS 서비스(레거시 보안 아키텍처에 비해 최대 40% 빠름)을 활용하여 생산성을 제고하고 조직의 민첩성을 개선합니다.
- **보안 아키텍처의 현대화:** 상당한 비용이 소요될 뿐만 아니라, 복잡하고 느린 기기의 90%를 완전히 클라우드 네이티브인 제로 트러스트 플랫폼으로 교체하는 등 Zscaler를 도입하면 ROI 139%를 달성할 수 있습니다.

오늘날의 하이브리드형 인력 운영 구조에 맞는 보안을 일관성 있게 제공하는 동급 최강의 플랫폼: 보안을 클라우드로 마이그레이션 단행할 경우, ID 및 컨텍스트를 이용하여 모든 사용자, 앱, 장치 및 위치를 위협으로부터 상시 보호할 수 있습니다. 즉, 보안 플랫폼이 사용자가 가는 모든 곳이라면 어디든 따라가는 체계를 도입할 수 있습니다.

별도의 인프라가 필요 없는 초고속 액세스: 직접적인 클라우드 액세스가 가능한 아키텍처는 빠르고 원활한 사용자 경험을 보장합니다. 이러한 구조는 특히, 백홀을 방지하고 성능과 사용자 경험을 개선하는 동시에 물리적 인프라 없이 네트워크 관리를 간소화합니다.

세계 최대 보안 클라우드를 활용한 AI 기반 보호: 하루 300조 건에 달하는 신호를 비롯한 위협 관련 인텔리전스를 기반으로 랜섬웨어, 피싱, 제로 데이 맬웨어, 지능형 공격 등을 차단하는 AI 기반 클라우드 보안 서비스 제품군을 사용하면 SSL 암호 해독을 포함한 모든 인터넷 및 SaaS 트래픽에 대한 인라인 검사를 수행할 수 있습니다.

관리의 간소화: 별도로 관리할 하드웨어가 없는 AI 기반의 클라우드 네이티브 보안 솔루션으로서 간소화된 워크플로우와 각 조직에 맞게 수립할 수 있는 보안 정책 덕분에 각 부서는 오로지 전략적 목표를 달성하는 데 집중할 수 있는 귀중한 시간을 확보할 수 있습니다.

통합된 AI 기반의 보안 및 데이터 보호 서비스

Zscaler Internet Access에는 사이버 공격과 데이터 손실을 방지하는 데 큰 도움이 되는 포괄적인 AI 기반의 보안 및 데이터 보호 서비스 제품군이 포함되어 있습니다. 모든 기능이 클라우드를 통해 제공되는 Zscaler Internet Access의 SaaS 솔루션을 활용하면 부가적인 하드웨어나 긴 배포 주기 없이 새로운 기능을 추가할 수 있습니다. Zscaler Internet Access 도입 시, 사용 가능한 모듈은 다음과 같습니다:

- **클라우드 보안 웹 게이트웨이(SWG):** 2020 Gartner MQ SWG 부문 세계 유일의 리더가 제공하는 실시간 AI 기반 분석 및 URL 필터링 기능을 활용하면 랜섬웨어, 맬웨어 및 기타 지능형 공격을 제거하여 안전하고 빠른 웹 경험을 제공할 수 있습니다.
- **클라우드 액세스 보안 브로커(CASB):** 통합 CASB를 이용하면 클라우드 앱을 보호하여 SaaS 및 IaaS 환경 전반에서 데이터의 안전을 확보하고 위협 차단, 규정 준수 등의 역량을 보장할 수 있습니다.
- **클라우드 데이터 손실 방지(DLP):** 완전한 인라인 검사와 정확한 데이터 일치(EDM), 광학 문자 인식(OCR) 및 기계 학습 등 첨단 기술을 활용하면 이동 중에도 데이터를 안전하게 보호할 수 있습니다.

가트너 매직 쿼드런트 SSE 부분 리더로 선정된 Zscaler

Gartner

- **Zscaler 방화벽 및 클라우드 IPS:** 업계 최고의 보안 기술을 모든 포트와 프로토콜로 확장 적용하고 에지 및 브랜치 방화벽을 클라우드 네이티브 플랫폼으로 교체할 수 있습니다.
- **Zscaler 샌드박스:** AI 기반 격리 기술을 활용하면 웹 및 파일 전송 프로토콜 전반에 걸쳐 기존에는 없었거나 파악하기 어려웠던 맬웨어를 차단하고 실시간으로 모든 사용자를 대상으로 글로벌한 보호 기능을 일관성 있게 유지할 수 있습니다.
- **AI 기반 클라우드 브라우저 격리:** 사용자, 웹 및 SaaS 사이에 가상의 여유 공간인 에어 갭을 생성하면 웹 기반 공격을 무력화 시키고 데이터 손실을 방지할 수 있습니다.
- **디지털 경험 모니터링:** 각종 분석 및 문제 해결을 위한 애플리케이션, 클라우드 경로 및 엔드포인트 성능 메트릭에 대한 통합 조회 기능을 통하면 IT 운영 관련 오버헤드 비용을 줄이고 티켓 해결 속도를 개선할 수 있습니다.
- **Zero Trust Branch Connectivity:** 사용자, 서버, IoT/OT 장치를 위한 라우팅이 불가능한 지사 및 데이터 센터를 연결하여 위험과 복잡성을 줄입니다.
- **DNS 보안:** 전세계 어디에서나 모든 포트와 프로토콜에서 모든 사용자, 장치, 애플리케이션의 DNS 보안과 성능을 최적화합니다.

사용자 및 워크로드를 위한 Zscaler Internet Access

Zscaler Internet Access를 사용할 경우, 인터넷 또는 SaaS 대상에 접근하는 클라우드 워크로드의 위험을 제거할 수 있습니다. 특히, 워크로드가 VPN, 방화벽(가상 방화벽 포함), 또는 WAN 기술과 같은 레거시 네트워크 중심 도구를 통해 인터넷에 접근할 필요성을 없앰으로써 여러 보안 도구를 사용할 필요 없이 보안 사고를 방지하고 내부 이동을 예방하는 효과를 가져다 줍니다. ZIA의 포괄적인 보안 및 데이터 보호 관련 제품군을 워크로드에 도입하면, 단일 통합 플랫폼으로도 사용자 및 워크로드에 대한 제로 트러스트 보안을 통합 제공할 수 있습니다.

또한, ZIA를 Zscaler Private Access와 페어링할 시에는 업무용 앱 및 워크로드가 퍼블릭 클라우드에 있든 사설 데이터 센터에 있든 모든 업무용 앱과 워크로드를 대상으로 보호를 확장할 수 있습니다.

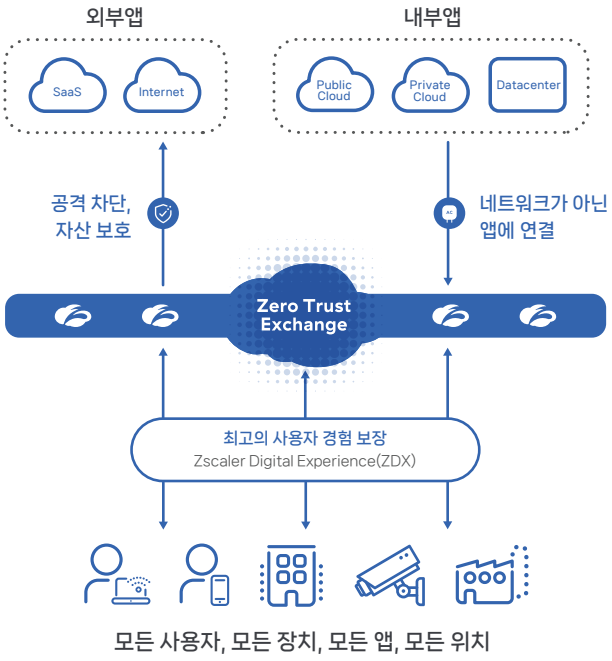

그림 1: The Zero Trust Exchange

사용 사례:

사이버 위협 및 랜섬웨어 공격에 대한 보호

기존의 레거시 네트워크 보안 체계를 대신해 Zscaler의 혁신적인 제로 트러스트 플랫폼을 도입할 경우, 각종 피해 예방, 공격 대상 제거, 위협 내부 전파 방지, 데이터 보호 등의 효과를 기대할 수 있습니다.

안전한 하이브리드 인력 운영 구조 확보

임직원, 협력사, 고객 및 공급업체가 위치나 사용 장치에 관계없이 웹 애플리케이션과 클라우드 서비스에 안전하게 액세스하고 최고의 디지털 경험을 누리도록 지원할 수 있습니다.

데이터 보호

실수로 인한 노출, 데이터 도난, 또는 이중으로 자산을 갈취하는 랜섬웨어로 인한 사용자, SaaS 앱 및 퍼블릭 클라우드 인프라의 데이터 손실을 예방할 수 있습니다.

인프라의 현대화

에지 및 브랜치 방화벽을 요하지 않는 빠르고 안전한 다이렉트 클라우드 액세스를 활용하면 비용을 대폭 절약하고 복잡한 네트워크 구조까지 간소화 할 수 있습니다.

Zscaler Zero Trust Exchange의 에코시스템

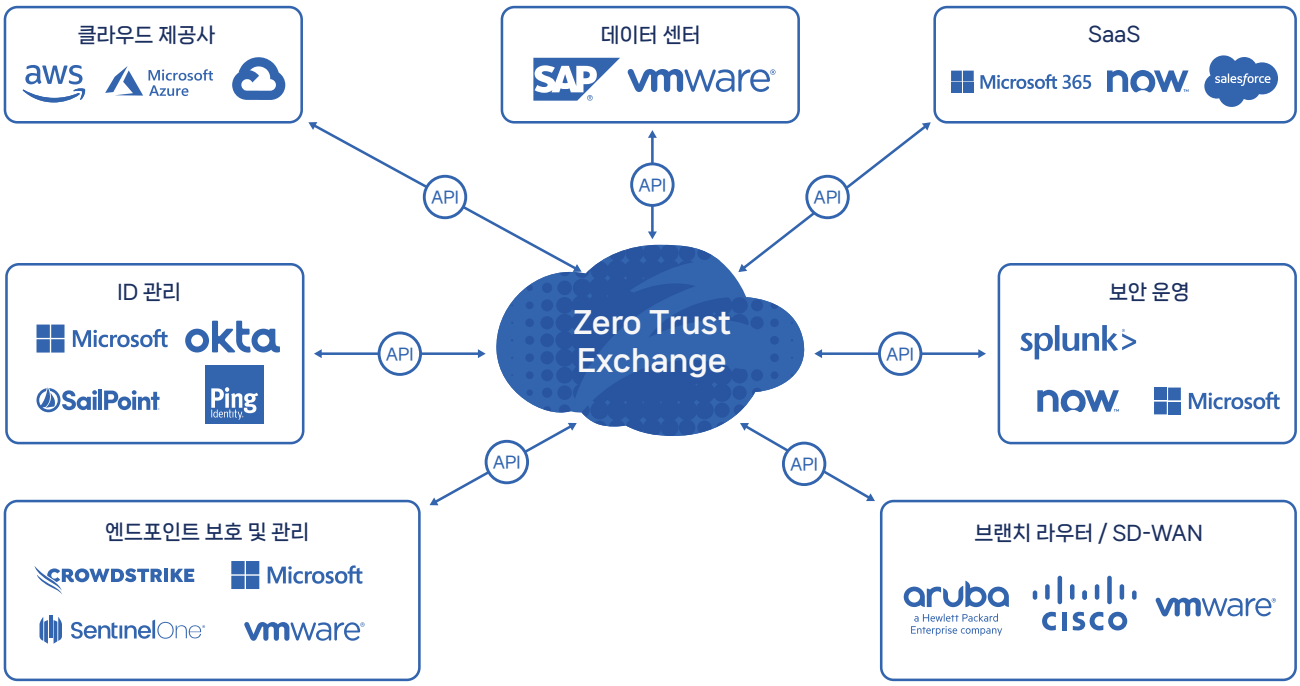

그림 2: Zscaler Internet Access 파트너 에코시스템

ZSCALER INTERNET ACCESS의 특징 및 기능	
특징	세부
기능	
URL 필터링	지정된 웹 카테고리 또는 대상에 대한 사용자 액세스를 허용, 차단, 주의, 또는 격리함으로써 웹 기반 위협을 차단하고 조직의 보안 정책을 준수하도록 지원합니다.
SSL 검사	무제한 TLS/SSL 트래픽 검사를 통해 암호화된 트래픽에 숨어 있는 위협 및 데이터 손실을 식별합니다. 개인 정보 보호 또는 규제 요건에 의거 검사해야 하는 웹 카테고리 또는 앱을 지정합니다.
DNS 보안	의심스러운 명령이나 제어 연결을 식별하고 Zscaler 위협 탐지 엔진에 라우팅하여 전체 콘텐츠를 검사합니다.
파일 제어	앱, 사용자, 또는 사용자 그룹에 따라 애플리케이션에 대한 파일 다운로드/업로드를 차단하거나 허용합니다.
대역폭 제어	대역폭 관련 정책을 시행하고 레크리에이션 트래픽보다 조직 활동에 크리티컬 한 애플리케이션에 우선 순위를 부여합니다.
고급 위협 보호	자사 독점 지능형 위협 보호 기능을 활용하여 맬웨어, 랜섬웨어, 공급망 공격, 피싱 등 지능형 사이버 공격을 차단합니다. 조직의 위험 허용 범위를 기반으로 세분화된 정책을 수립합니다.
인라인 데이터 보호 (이동 데이터)	정방향 프록시 및 SSL 검사 기능을 활용하여 위험한 웹 대상 및 클라우드 앱으로 향하는 민감 정보의 흐름을 실시간으로 제어함으로써 데이터에 대한 내외부 위협을 차단합니다. 앱의 승인 여부와 관계없이 네트워크 장치 로그를 요구하지 않고 고급 인라인 보호 기능이 제공됩니다.
대역 외 데이터 보호 (저장 데이터)	SaaS 앱, 클라우드 플랫폼 및 해당 콘텐츠를 스캔할 수 있도록 API 통합을 사용하여 저장되어 있는 민감 데이터를 식별하고 위험하거나 외부 공유를 중단함으로써 자동으로 문제를 해결합니다.
침입 방지	각종 사용자, 앱 및 위협에 대한 컨텍스트 정보를 수집하고 봇넷, 지능형 위협 및 제로-데이 맬웨어로부터 시스템을 완벽하게 보호합니다. 클라우드 및 웹 IPS는 클라우드 방화벽, 클라우드 샌드박스, 클라우드 DLP, CASB에서 원활히 작동합니다.
동적 위험 기반 액세스 및 보안 정책	사용자, 장치, 애플리케이션 및 콘텐츠 위험에 따라 보안 및 액세스 정책을 자동으로 조정합니다.
트래픽 캡처	원활한 패킷 캡처: Zscaler 정책 엔진 내에서 특정 기준을 통해 암호화된 트래픽을 손쉽게 캡처하여 추가 기기 없이도 효율적인 보안 포렌식을 지원합니다.
맬웨어 분석	고급 AI/ML 기술을 이용해 악성 페이로드에 숨어 있는 알려지지 않은 위협을 탐지, 예방 및 격리하여 페이션트 제로 공격을 차단합니다.
DNS 필터링	알려진 대상 및 악성 대상의 DNS 요청을 제어하고 차단합니다.
웹 격리	활성 콘텐츠를 무해한 픽셀 스트림의 형태로 최종 사용자의 브라우저에 전달함으로써 웹 기반 위협의 위험성을 제거합니다.
관련 위협에 대한 인사이트	위협 점수, 노출 대상(자산), 피해의 심각도 등에 대한 정보를 활용하여 상황에 맞는 경고를 제공함으로써 조사 및 응답 시간을 단축합니다.
애플리케이션 격리	중요한 데이터의 손실을 방지하기 위해 복사/붙여넣기, 업로드/다운로드 및 출력 등 사용자 작업을 세세히 제어하여 SaaS, 클라우드 및 업무용 앱을 대상으로 안전하고 별도의 관리가 필요하지 않은 에이전트리스 장치 액세스를 보장합니다.
디지털 경험 모니터링	분석 및 문제 해결을 위해 애플리케이션, 클라우드 경로 및 엔드포인트 성능 메트릭 정보를 통합 조회합니다.
Zero Trust Branch Connectivity	Zero Trust Exchange를 통해 지점간 연결을 현대화하여 공격 대상을 제거하고 내부 전파를 방지합니다.
워크로드-인터넷 통신 보호	워크로드와 인터넷 간 통신을 위해 피해를 예방하고 위협의 내부 전파를 방지합니다. 이때, SSL 검사, IPS, URL 필터링 및 모든 통신에 대한 데이터 보호가 포함됩니다.
IoT 장치 가시성	자동화된 검색, 지속적인 모니터링, 업계 최고의 자동 라벨링 기능을 통한 AI/ML 분류를 통해 비즈니스 전반의 모든 IoT 장치, 서버, 관리되지 않는 사용자 장치를 완벽하게 파악할 수 있습니다.

특징	세부
플랫폼 기능	
유동적인 연결 옵션	• **Zscaler Client Connector(ZCC):** Windows, macOS, iOS, iPadOS, Android 및 Linux를 지원하는 경량 에이전트를 통해 Zero Trust Exchange로 트래픽을 전달합니다. • **GRE 또는 IPsec 터널:** ZCC가 없는 장치를 대상으로 GRE 및/또는 IPsec 터널을 통해 Zero Trust Exchange로 트래픽을 전달합니다. • **브라우저 격리:** 통합 Cloud Browser Isolation 기능으로 모든 BYOD 또는 관리되지 않는 장치를 원활하게 연결합니다. • **프록시 체이닝:** Zscaler는 한 프록시 서버에서 다른 프록시 서버로의 트래픽 전달을 지원하나, 프로덕션 환경에서는 권장되지 않습니다. • **PAC 파일:** ZCC가 없는 장치를 대상으로 PAC 파일을 사용하여 Zero Trust Exchange로 트래픽을 전달합니다.
클라우드 배포	SaaS로 제공되는 100% 클라우드 네이티브 플랫폼입니다. 특이 사례의 경우, 프라이빗 및 가상 서비스 에지를 선택할 수 있습니다.
데이터 보호 및 보존	데이터를 로깅할 때 콘텐츠는 디스크에 기록되지 않으며, 로깅이 구체적으로 수행되는 위치를 결정할 때에는 세분화된 제어 체계를 활용합니다. 주요 준수 규정에 의거, 역할 기반 액세스 제어(RBAC)를 사용하여 읽기 전용 액세스, 사용자 이름 익명화/난독화, 부서 또는 기능별 액세스 권한을 부여합니다. 데이터는 제품에 따라 6개월 이하의 기간 동안 유지됩니다. 데이터를 보관하기 위한 추가 스토리지는 원하는 기간 만큼 구입할 수 있습니다.
주요 준수 규정 관련 인증	인증에는 다음이 포함됩니다: • FedRAMP • ISO 27001 • SOC 2 Type II • SOC 3 • NIST 800-63C 준수 규정 관련 인증의 전체 목록은 이곳에서 확인하실 수 있습니다.
세분화된 API 지원	당사는 각종 ID, 네트워킹 및 보안 서비스 공급업체와의 REST API 통합을 유지 관리합니다. 예를 들어, Zscaler와 클라우드 기반 또는 온프레미스 SIEM(예시: Splunk) 간에 로그를 공유할 수 있습니다.
다이렉트 피어링	주요 인터넷 및 SaaS 제공사 및 퍼블릭 클라우드 대상과의 다이렉트 피어링은 최대한 빠른 트래픽 경로를 확보합니다.
서비스 레벨 계약(SLA)	
가용성	99.999%, 트랜잭션 손실로 측정
프록시 레이턴시	< 100ms, 위협 및 DLP 검사가 활성화 되어 있는 경우 포함
바이러스 캡처	알려진 바이러스 및 맬웨어의 100%
지원 플랫폼 및 시스템	
Client Connector	최소 요구 사양: • iOS 9 이상 • Android 5 이상 • Windows 7 이상 • Mac OS X 10.10 이상 • CentOS 8 • Ubuntu 20.04
Branch Connector	최소 요구 사양: • VMware vCenter 또는 vSphere Hypervisor • Centos • Redhat

ZIA 에디션

	ZIA Essentials Edition	ZIA Business Edition	ZIA Transformation Edition	ZIA Unlimited Edition
Platform Services	Content Filtering Inline AV, TLS/SSL Inspection, Nanolog Streaming	Content Filtering Inline AV, TLS/SSL Inspection, Nanolog Streaming	(+) Cloud NSS, NSS Log recovery, Extended DC Access, IPSec Tunnel, Contextual Alerts, ZIA Virtual Private Service Edge(8)	(+) Source IP Anchoring, Test Environment, Priority Categorization, ZIA Virtual Private Service Edge(32), Server & IoT Protection(1GB/10 users)
Advanced Threat Protection (incl. AI-powered phishing & C2 detection)	✓	✓	✓	✓
Cloud Sandbox with AI powered quarantine	Add-on	Add-on	✓	✓
AI-powered Risk-based Isolation	Add-on	Add-on	Standard (100MB/user/mo.)	Advanced Plus (1500MB/user/mo.)
Correlated Threat Insights	—	✓	✓	✓
Dynamic Risk-based Policy	—	—	✓	✓
Integrated Deception	—	—	Standard (min 1000 ZIA licenses req)	Standard (min 1000 ZIA licenses req)
DNS Resolution & Filtering	upto 64 rules	upto 64 rules	✓	✓
DNS Tunnel Detection	—	—	✓	✓
Bandwidth Control	—	✓	✓	✓
Cloud Firewall	Network, Application Services, Locations, FQDNs upto 10 rules	Network, Application Services, Locations, FQDNs upto 10 rules	(+) work from anywhere users, locations, deep packet application inspection	(+) work from anywhere users, locations, deep packet application inspection
Protection for unauthenticated Traffic	0.5GB/user/mo.	1GB/user/mo.	1.5GB/user/mo.	2GB/user/mo.
Cloud App Control + Tenancy Restrictions	✓	✓	✓	✓
Isolation for SaaS Apps	Add-on	Add-on	Standard (100MB/user/mo.)	Advanced Plus (1500MB/user/mo.)
Data Loss Prevention, CASB, Inline Web Essentials, SaaS API (1 app)	—	Data Protection Std. (DLP and CASB Essentials)	(+) SaaS API Retro Scan	✓
SaaS API, App Total, Unmanaged Devices, Classification, Incident Management	Add-on	Add-on	Add-on	✓
Digital Experience Monitoring	—	Standard	Standard	Standard
Premium Support Plus	Add-on	Add-on	Add-on	✓

라이선스 모델

모든 Zscaler Internet Access 에디션의 가격은 사용자당 요율을 기준으로 책정됩니다. 각 에디션에 포함된 특정 제품의 경우, 가격은 사용자 수 이외에 다른 요인에 의해 조정될 수 있습니다. 가격 책정에 대한 자세한 내용은 Zscaler 담당 팀에 문의해 주시기 바랍니다.

Zero Trust Exchange 호환 플랫폼

Zero Trust Exchange를 사용하면 빠르고 안전한 연결이 가능하며, 임직원은 회사 네트워크를 인터넷으로 활용하여 언제, 어디서나 주어진 업무를 수행할 수 있습니다. 더불어, 최소 권한으로 액세스를 제어하는 제로 트러스트 원칙을 바탕으로 컨텍스트 기반 ID 및 정책 시행을 통해 포괄적인 보안 기능을 제공합니다.

지스케일러 코리아 hlee@zscaler.com | www.zscaler.com

zscaler™
Experience your world, secured.™

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134