Zscaler Zero Trust SASE

AT-A-GLANCE

Zero Trust SASE의 이점

비용 절감 및 복잡성 완화
운영상의 마찰과 비용을 절감하기 위해, 여러 개의 개별 제품을 통합 정책 엔진과 관리 콘솔을 갖춘 하나의 통합 플랫폼으로 통합하세요.

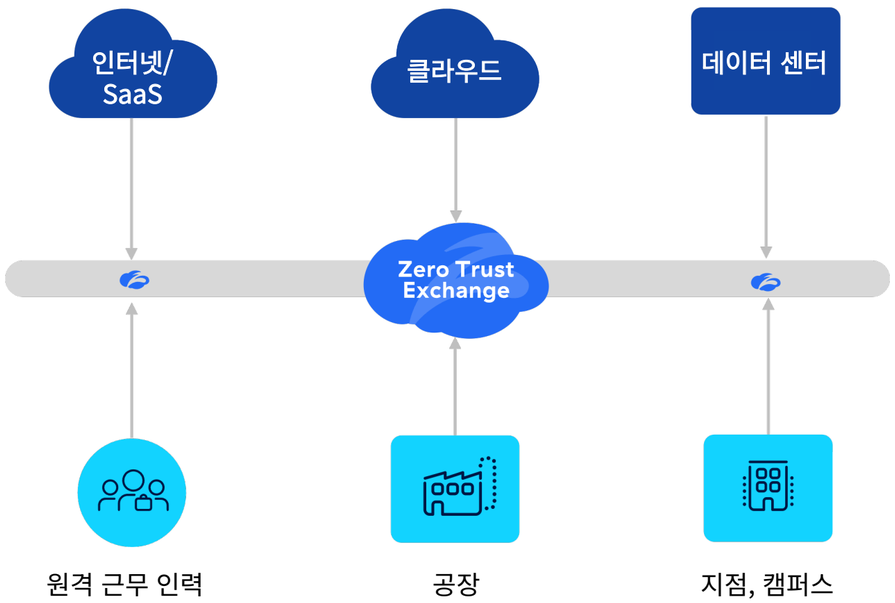
탁월한 보안
공격 표면을 제거하고 진정한 Zero Trust 방식으로 측면 위협 확산을 차단하세요. 기존 방화벽을 적응형 액세스 및 AI 기반 보안으로 대체하여 모든 트래픽을 보호하세요.

사용자 경험 향상
클라우드 마이그레이션을 가속화하고 불필요한 트래픽 백홀을 제거하여 본사부터 커피숍까지 모든 위치에서 사용자 경험을 최적화하세요.

향상된 비즈니스 민첩성
기존 네트워크의 제약 없이 신속하게 확장하세요. 사용자를 조직 간 비즈니스 앱에 직접 연결하여 M&A 통합을 가속하고 며칠 내에 가치를 실현하세요.

Zscaler Zero Trust SASE: 통합 브랜치, SSE 및 AI 보안

Zscaler Zero Trust SASE™는 사용자와 지점을 클라우드 애플리케이션에 안전하게 연결하는 클라우드 네이티브 플랫폼입니다. Zscaler는 공격 표면을 제거하고 측면 이동을 방지함으로써 레거시 방화벽 기반 접근 방식을 대체하는 시장 유일의 진정한 Zero Trust SASE 솔루션을 제공합니다.



Security Service Edge(SSE)
- 사이버 위협 보호
- 데이터 보안
- 제로 트러스트 액세스
- AI 보안

제로 트러스트 네트워킹
- Zero Trust Branch
- Zero Trust Cloud
- Digital Experience
- Zscaler Cellular

Zscaler Zero Trust SASE를 사용하는 이유

✓ 세계 최대 규모의 AI 보안 클라우드가 제공하는 최고 수준의 사이버 위협 보호 및 데이터 보안

✓ 160개 이상의 글로벌 데이터 센터를 통해 제공되며 데이터 주권 제어 기능을 갖춘 클라우드 네이티브 플랫폼

✓ 공격 표면을 축소하고 측면 이동 위험을 제거하는 차별화된 제로 트러스트 아키텍처

Zero Trust SASE: 주요 기능

Zero Trust SASE 플랫폼

하루 5천억 건 이상의 거래를 처리하는 세계 최대 규모의 AI 보안 클라우드인 Zscaler의 Zero Trust Exchange를 기반으로 하는 Zero Trust SASE는 사용자, IoT/OT 기기, AI 에이전트 및 클라우드 앱을 안전하게 연결합니다.

- **공격 표면 없음:** AI 기반 위협으로부터 노출 및 침해를 방지합니다.
- **암묵적 신뢰 배제:** 측면 이동을 차단하고 피해 범위를 최소화합니다.
- **어디서나 제로 트러스트:** 사용자를 위한 통합 보호 IoT/OT, 그리고 모든 지역의 워크로드를 관리합니다.
- **AI 기반 보안:** 업계 최대 규모의 데이터 세트를 활용하여 적응형 접근 제어 및 위협 보호 기능을 제공합니다.
- **디지털 경험:** 최적화된 성능을 위한 AI 기반 문제 해결 및 원격 측정 기능.

Security Service Edge(SSE) 기능

Zscaler의 SSE는 통합 프록시 아키텍처를 통해 포괄적인 보호 기능을 제공하여 웹, 클라우드 서비스 및 개인 애플리케이션에 일관된 보안을 보장합니다. 주요 기능:

- **보안 웹 게이트웨이(ZIA):** AI 기반 멀웨어 방지, 고급 샌드박싱 및 동적 대역폭 제어 기능을 갖춘 완벽한 프록시 검사 기능.
- **제로 트러스트 네트워크 액세스(ZPA):** 앱을 인터넷으로부터 숨겨 기존 VPN을 대체하고 측면 이동을 방지하는 ID 기반 Zero Trust 적응형 액세스.
- **데이터 보안:** 모든 데이터 손실 경로에 대한 가시성과 보호 기능을 제공하며, 고급 AI 분류, CASB, 데이터 보안 태세 관리(DSPM)를 검증된 인라인 DLP와 통합.

Zero Trust Branch

Zscaler Zero Trust Branch는 제로 트러스트 아키텍처를 사용하여 사이트를 안전하게 연결하고, 복잡한 라우팅 및 방화벽을 없애는 동시에 사용자와 IoT/OT 기기의 측면 이동을 방지합니다. 주요 기능:

- **고성능 연결:** 2Gbps에서 40Gbps까지 확장 가능한 처리량.
- **에이전트리스 세분화:** IoT/OT의 측면 이동을 차단하는 네이티브 마이크로세분화.
- **가시성:** 추가 하드웨어나 에이전트 없이 자산 탐색 및 트래픽 프로파일링 자동화.

고급 AI 보안

Zscaler는 새로운 AI 기반 위협으로부터 보호하는 동시에 안전한 GenAI 도입을 가능하게 하는 완벽한 AI 보안 프레임워크를 제공합니다.

- **AI 자산 관리:** Gen AI 앱, LLM, 모델, MCP 서버 및 파이프라인을 포함한 모든 AI 환경에 대한 포괄적인 가시성을 제공하여 노출 및 취약점을 정확히 파악할 수 있도록 지원합니다.
- **AI 접근 보안:** 세분화된 접근 제어 및 DLP 보호 기능을 통해 AI 애플리케이션의 안전한 사용을 보장하고 기업 정책 준수를 확보합니다.
- **모델 보안(SPLX):** 내부 AI 애플리케이션 수명주기를 보호하기 위해 고급 AI 레드티밍 및 위협 검사를 통합합니다.

©2026 Zscaler, Inc. 모든 권리 보유.

Zscaler Zero Trust SASE: 기능 개요

위협 보호	웹, SaaS 및 개인 애플리케이션 전반에 걸쳐 AI 기반 멀웨어 방지 및 고급 샌드박싱 기능을 갖춘 완벽한 프록시 검사 기능을 제공합니다. 실시간 위협 방지, AI 기반 피싱 탐지 및 Zero Trust 기능을 포함합니다.
적응형 액세스	AI 및 제3자 신호를 기반으로 한 실시간 위험 점수를 활용하는 동적이고 신원 기반의 접근 제어. 적응형 액세스 엔진은 단계별 인증 또는 브라우저 격리를 포함하여 액세스 권한을 동적으로 조정합니다.이 시스템은 사용자 개체 행동 분석(UEBA)을 사용하여 불가능한 이동이나 대량 업로드와 같은 이상 징후를 감지합니다.
인라인 온프레미스 보안 제어	Zero Trust Branch는 복잡하고 라우팅 가능한 SD-WAN을 대체하고 기존 VPN 및 방화벽을 제거합니다. 이 솔루션은 관리되지 않는 IoT 및 OT 장치에 대해 에이전트리스 방식의 마이크로세그멘테이션을 제공하여 지점 및 공장 내에서의 측면 이동을 차단합니다.
프라이빗 애플리케이션 보안 강화	Secure Private Access(ZPA)는 모든 연결을 Zero Trust Exchange를 통해 중개하고 ID 기반 Zero Trust 제어를 적용하여 개인 애플리케이션(API 및 워크로드 포함)을 인터넷으로부터 숨깁니다. 수신 포트가 없는 경량 앱 커넥터를 사용하여 공격 표면을 줄이고 침해를 방지합니다.AppProtection은 OWASP Top-10 및 사용자 지정 서명을 사용하여 페이로드를 검사합니다.
SaaS 제어 및 가시성	클라우드 프록시(인라인) 및 API 통합(대역 외 CASB)을 통한 통합 가시성 및 제어 기능으로 특정 승인되거나 승인되지 않은 앱에 대한 액세스를 허용, 차단 또는 격리하는 세분화된 제어가 가능합니다. 이 서비스는 플러그인과 코드를 포함하여 9만 개 이상의 SaaS 앱에 대한 포괄적인 위험 평가를 제공합니다.
데이터 보안	Zero Trust SASE는 데이터 보안에 대한 통합적인 접근 방식을 제공하여 모든 데이터 손실 경로에 걸쳐 가시성과 보호 기능을 확장합니다. Zscaler는 Advanced AI Classification과 Data Security Posture Management(DSPM)를 검증된 인라인 DLP와 통합하여 어디서나 모든 데이터를 포괄적으로 제어할 수 있도록 합니다.
AI Security	AI 앱을 위한 인라인 검사 기능을 갖춘 완벽한 AI 보안 프레임워크입니다. AI Guard & Prompt Inspection은 프롬프트 입력과 파일 업로드를 통해 데이터 유출을 방지합니다. AI 라이프사이클 보안(AI-SPM, AI Red Teaming, AI Guardrails) 및 통합 AI 자산 인벤토리를 완벽하게 제공합니다.

©2026 Zscaler, Inc. 모든 권리 보유.

SD-WAN	Zero Trust SD-WAN은 복잡하고 라우팅 가능한 SD-WAN을 제로 트러스트 오버레이로 대체합니다. 주요 기능으로는 지능형 앱 인식 트래픽 제어, BGP 및 OSPF와 같은 라우팅 프로토콜 지원, 중앙 집중식 가시성 및 관리, ZT Branch 어플라이언스용 제로 터치 프로비저닝 등이 있습니다.
커피숍 네트워킹	Zero Trust SASE는 사용자의 위치에 관계없이 간소화되고 일관된 경험을 제공하여 네트워크 복잡성을 최소화하고 어디서든 빠르고 일관된 환경을 보장합니다. Zscaler의 "카페형 지점" 개념은 지점 방화벽과 네트워크 라우팅의 복잡성을 없애는 혁신적인 접근 방식입니다.
통합 플랫폼	단일 클라우드 네이티브 제로 트러스트 익스체인지 플랫폼은 웹, SaaS 및 프라이빗 애플리케이션 전반에 걸쳐 보안을 위한 통합 프록시 아키텍처를 제공합니다. 이 시스템은 모든 서비스(보안 및 네트워킹)에 걸쳐 통합 정책 엔진과 관리 콘솔을 사용하여 워크플로를 간소화하고 운영상의 마찰을 줄입니다.
기업 통합	Zscaler의 Zero Trust SASE는 150개 이상의 기술 파트너(SIEM, SOAR, EDR, ITSM)와 강력한 API 기반 통합 기능을 제공합니다. Nanolog Streaming Service(NSS)는 원활한 에코시스템 협업을 위해 모든 수신자에게 로그를 푸시합니다.
디지털 경험	Integrated Digital Experience(ZDX) 모니터링은 앱, ZIA/ZPA, 인터넷 서비스 제공업체(ISP) 및 기기 전반에 걸쳐 AI 기반 근본 원인 분석을 제공합니다.
주권 통제	특정 지역의 주권 요건을 충족하기 위해 데이터 평면, 제어 평면 및 관리 평면에 대한 세부적인 조직 제어 기능을 제공합니다. 트래픽 라우팅, 검사, 로그 및 관리 플레인의 호스팅 위치를 제어할 수 있습니다.

Zero Trust SASE에 대해 더 자세히 알아보려면 zscaler.com/capabilities/secure-access-service-edge를 방문하여 네트워크 없이 구현하는 네트워크 보안의 미래를 확인해 보세요.

Zscaler 소개

Zscaler(NASDAQ: ZS)는 고객이 더욱 민첩하고 효율적이며 탄력적이고 안전하게 디지털 전환을 가속화할 수 있도록 지원합니다. Zscaler Zero Trust Exchange™ 플랫폼은 위치에 관계없이 사용자, 장치 및 애플리케이션을 안전하게 연결하여 수천 개의 고객사를 사이버 공격과 데이터 손실로부터 보호합니다. 전 세계 150개 이상의 데이터 센터에 분산된 SSE 기반 Zero Trust Exchange™는 세계 최대 규모의 인라인 클라우드 보안 플랫폼입니다. 자세한 내용은 **zscaler.com**에서 확인하거나 X에서 **@zscaler**를 팔로우하세요.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™ 및 **zscaler.com/legal/trademarks**에 명시된 기타 상표는 (i) 미국 및/또는 기타 국가에서 Zscaler, Inc.의 등록 상표 또는 서비스표이거나 (ii) Zscaler, Inc.의 상표 또는 서비스표입니다. 기타 모든 상표는 해당 소유자의 자산입니다.

+1 408.533.0288 **Zscaler, Inc. (본사) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Zero Trust Everywhere