ZPA

Zscaler Private Access™

모든 사용자, 장치 및 위치를 대상으로 빠르고 안전하게

업무용 애플리케이션에 다이렉트 액세스를 제공하는 플랫폼

zscaler™

Zscaler Private Access

모든 사용자, 장치 및 위치를 대상으로 빠르고 안전하게 업무용 애플리케이션에 다이렉트 액세스를 제공하는 플랫폼

업계 유일의 차세대 제로 트러스트 네트워크 액세스(ZTNA) 플랫폼인 Zscaler Private Access (ZPA)는 오늘날의 하이브리드형 인력 운영 구조에 맞는 새로운 개념의 업무용 앱(기업의 업무용 애플리케이션) 연결 및 보안 기능을 제공합니다.

최근 떠오르는 하이브리드형 인력 운영 구조의 니즈를 충족하지 못하는 레거시 네트워킹 및 보안 접근 방식

사용자를 업무용 앱에 연결할 때, 속도가 느리거나, 복잡하고 위험한 방식은 반드시 지양해야 합니다. 하이브리드형 업무 방식의 도입과 클라우드 서비스의 보급 덕분에 각종 기업 업무용 애플리케이션은 클라우드로 마이그레이션이 이루어지고 있으며, 애플리케이션 사용자들 또한 다양한 장치와 퍼블릭 인터넷을 활용해 원하는 장소에서 애플리케이션에 접속할 수 있게 되면서 경계 기반 네트워크 보안 모델에 큰 변화의 바람이 불고 있습니다. 애플리케이션 액세스를 제어하기 위해 레거시 VPN 및 방화벽에 의존하던 기존 접근 방식의 경우, 클라우드 및 모바일 플랫폼이 우선인 환경에서는 효율성이 떨어집니다.

가트너 발표에 따르면, 2025년까지 새로 보급될 원격 액세스 애플리케이션의 70% 이상은 VPN 서비스와 달리 제로 트러스트 네트워크 액세스(ZTNA)를 통해 주로 제공될 전망(2021년 말 : 10% 미만)입니다.

특장점:

- **하이브리드형 인력 운영 체제의 생산성 향상**
  자택, 사무실, 또는 원하는 장소에서 업무용 앱에 빠르고 원활하게 액세스할 수 있습니다.
- **데이터 침해의 위험 경감**
  최소 권한 액세스 체계를 적용하여 공격자에게 애플리케이션을 노출시키지 않음으로써 공격 대상을 최소화하고 위협 내부 전파를 방지할 수 있습니다.
- **최신 위협 차단**
  업계 최초로 선보이는 업무용 앱 보호 기능으로 위험 사용자 및 공격을 시도하는 공격자로 인한 위험을 최소화 할 수 있습니다.
- **앱, 워크로드 및 장치 전반에 걸쳐 제로 트러스트 확장 적용**
  세계에서 가장 완벽한 성능을 자랑하는 ZTNA 플랫폼을 활용하면, 업무용 앱, 워크로드 및 OT/IIoT 장치를 최소 권한 액세스 체계를 통해 보호할 수 있습니다.
- **운영 복잡성 감소**
  클라우드 네이티브 플랫폼을 활용하면 확장, 관리 및 구성이 복잡하고 까다로운 레거시 VPN을 제거할 수 있습니다.

레거시 네트워크 보안 접근 방식의 경우, 공격자는 기존의 '성과 해자(castle-and-moat)' 형태의 아키텍처에 대한 맹목적인 신뢰와 지나치게 광범위한 액세스 권한을 악용하여 보안 조치를 손쉽게 우회할 수 있습니다. 레거시 네트워크 보안은 다음과 같이 여러 가지 약점을 지니고 있습니다:

- **레거시 아키텍처는 확장이 어렵고 빠르고 원활한 사용자 경험을 제공할 수 없습니다:** VPN은 백홀을 요하는데, 백홀은 최근 늘어난 원격 업무 구조에 상당한 비용 부담으로 작용하고 복잡성과 대기 시간 또한 증가시킵니다.
- **기존 방화벽, VPN 및 업무용 앱은 대규모 공격의 대상이 됩니다:** 공격자는 보안이 취약하고 외부에 노출된 리소스를 확인하고 악용할 수 있습니다.
- **최소 권한 액세스 체계를 사용하지 않기 때문에 내부 이동이 자유롭습니다:** VPN은 사용자를 네트워크에 연결하여 공격자가 민감한 데이터에 쉽게 액세스할 수 있도록 합니다.
- **위험 사용자 및 조직 내부의 위협은 기존 제어 조치를 피해갈 수 있습니다:** 실력이 우수한 공격자는 레거시 원격 액세스 도구 및 1세대 ZTNA 제품을 사용하여 업무용 앱에 액세스하기 위해 자격 증명을 훔치고 ID를 도용할 수 있습니다.

이제는 사용자를 필요한 애플리케이션에 안전하고 원활하게 연결할 수 있는 방법을 새롭게 고민해 보아야 할 때인 만큼 차세대 제로 트러스트 네트워크 액세스로 기업의 업무용 애플리케이션 보안 체계의 도입을 검토해 보아야 합니다.

Zscaler Private Access

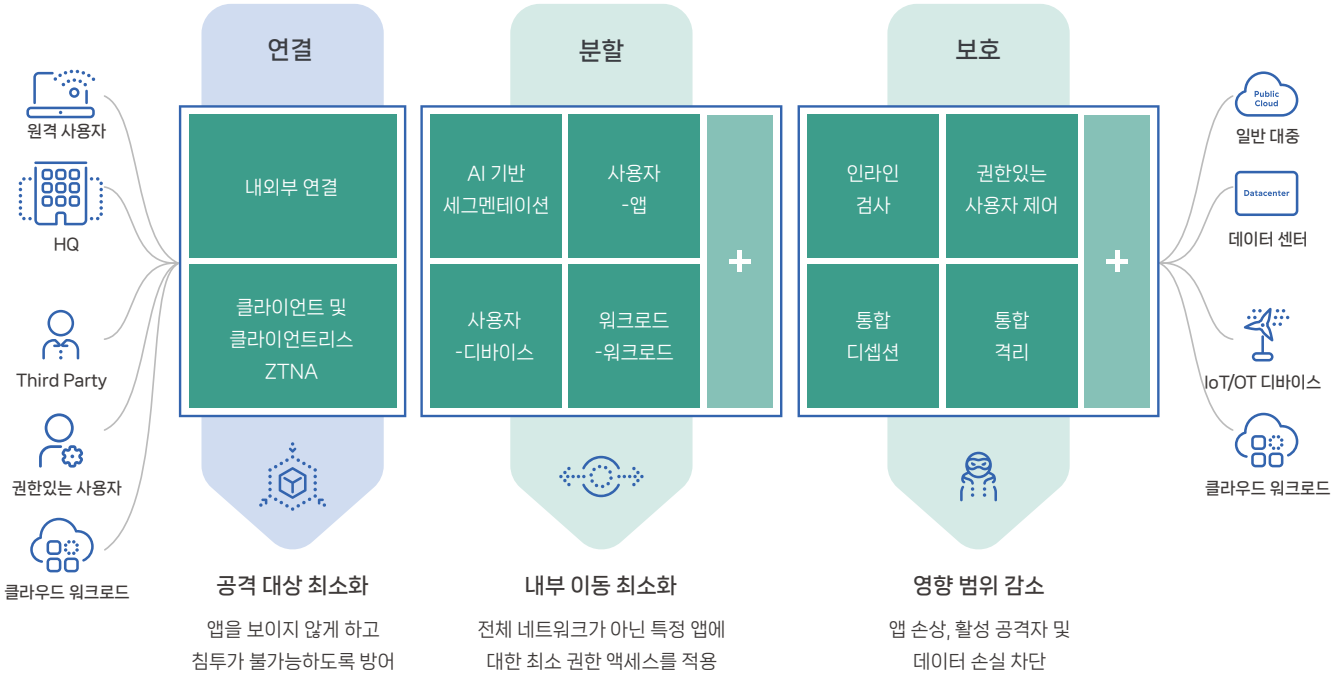
ZPA는 세계에서 가장 널리 배포된 ZTNA 플랫폼으로, 최소 권한 원칙을 적용하여 사용자를 온프레미스 또는 퍼블릭 클라우드에서 실행되는 업무용 애플리케이션에 안전하게 연결(직접 연결) 시켜주는 동시에 무단 액세스 및 위협 내부 전파까지 방지합니다. 전체적인 보안 서비스 에지(SSE) 프레임워크를 기반으로 구축된 클라우드 네이티브 서비스인 ZPA의 경우, 단 몇 시간이면 준비가 모두 완료되며 레거시 VPN 및 원격 액세스 도구를 대체하여 다음과 같은 기능을 즉시 수행할 수 있습니다:

- **우수한 사용자 경험 제공:** 사용자를 업무용 앱에 직접 연결하면 기존 VPN을 통한 느리고 값비싼 백홀 단계를 제거하는 한편, 사용자 경험 관련 문제를 지속적으로 모니터링하고 사전에 해결할 수 있습니다.
- **공격 대상 최소화:** 애플리케이션은 인터넷과 권한이 없는 사용자에게는 전혀 보이지 않으며, IP가 내외부 연결을 통해 노출될 우려도 없습니다.
- **최소 권한 액세스 적용:** 애플리케이션에 대한 액세스는 IP 주소가 아닌 ID와 컨텍스트에 따라 결정되며, 사용자가 액세스를 위해 네트워크에 연결되는 일은 없습니다.
- **위협 내부 전파 방지:** 사용자가 특정 앱에만 액세스할 수 있도록 애플리케이션이 분할되어 내부 이동을 제한하는 데 도움이 됩니다.
- **완전한 검사로 공격 무력화:** 가장 널리 사용되고 있는 웹 공격 기술을 방지하기 위해 업무용 앱 트래픽을 인라인으로 검사합니다.

2025년까지 새롭게 배포된 원격 액세스 애플리케이션의 최소 70%는 주로 ZTNA (제로 트러스트 네트워크 액세스)를 통해 제공될 전망입니다.

Gartner®

Next-Generation ZTNA 기능



주요 사용 사례

VPN의 대안

레거시 VPN은 보안, 확장성 또는 사용자 경험을 염두에 두고 설계되지 않았습니다. 일반적으로 VPN은 모든 원격 사용자 트래픽을 수천 마일 떨어진 데이터 센터로 백홀하므로 대기 시간이 길어지고 사용자 불만을 초래합니다. 연결되면 VPN은 방화벽을 통과하여 사용자를 터널링하고 애플리케이션과 동일한 네트워크에 배치하여 자유로운 내부 이동을 허용합니다. ZPA는 VPN 고유의 백홀 대기 시간이나 보안 위험 없이 빠르고 안전한 원격 액세스를 제공하여 이러한 문제를 극복합니다. 내외부 연결을 통해 앱 액세스가 네트워크 액세스와 분리되고 권한이 있는 사용자만 지정된 앱에 액세스할 수 있으므로 내부 이동이 발생하지 않습니다.

ZPA의 클라우드 네이티브 멀티테넌트 설계는 IT 팀이 인바운드 게이트웨이 어플라이언스(방화벽, 로드 밸런서, DDOS 탐지 등)를 없애고 네트워크 비용과 복잡성을 줄일 수 있다는 것을 의미합니다.

안전한 하이브리드 인력 운영 구조 확보

최근 사용자들은 자택, 멀리 떨어져 있는 현장, 지사 및 본사 간에 유동적으로 이동하면서 사용할 수 있는 솔루션을 찾고 있습니다. ZPA를 사용하면 작업이 필요한 곳이라면 어디에서든 원하는 장치를 이용하여 업무용 앱에 원활하고 안전하게 액세스할 수 있습니다. 로컬 사용자 또한 클라우드의 모든 정책과 제어 조치를 복제하는 온프레미스 브로커를 통해 원격 사용자와 동일한 사용자 경험과 이점을 누릴 수 있습니다. 더불어, 디지털 경험 모니터링을 활용할 경우, 성능 저하 및 고장 등을 실시간으로 확인함으로써 보다 생산적으로 오늘날의 하이브리드형 인력 구조를 관리할 수 있습니다. Zscaler Zero Trust Exchange를 도입한 사용자는 인터넷, SaaS, 워크로드, 장치 및 업무용 앱에 안전하고 빠르게 직접 액세스할 수 있는 통합 SSE 플랫폼의 특장점을 충분히 누릴 수 있습니다.

Third-party 액세스 / VDI의 대안

과거에는 Third Party 액세스가 거추장스럽고 비용이 많이 드는 가상 데스크톱이나 RDP, SSH 또는 VNC와 같은 기타 원격 데스크톱 클라이언트를 통해 이루어졌기 때문에 사용자가 네트워크에 직접 접속하고 내부 시스템이 신뢰할 수 없는 장치에 노출되었습니다.

ZPA의 클라이언트리스 액세스 기능을 사용하면 Third Party 액세스가 웹에 액세스하는 것처럼 쉬워져 비용을 절감하고 위험을 최소화할 수 있습니다. 공급사, 도급업자 및 협력사는 클라이언트 없이도 자신의 디바이스에서 웹 브라우저를 자유롭게 사용하여 인트라넷 웹사이트, 내부 시스템 및 장비에 연결할 수 있습니다. Third Party 사용자와 관리되지 않는 디바이스를 네트워크 및 애플리케이션으로부터 격리하여 중요한 데이터가 통제 범위를 벗어나지 않도록 하고 무단 클립보드, 인쇄, 업로드/다운로드 등으로부터 보호할 수 있습니다. 클라이언트리스 액세스를 통해 IT 부서는 기존 가상 데스크톱 인프라(VDI)를 관리하는 데 드는 비용 없이 사용자에게 더 나은 보안 환경을 제공할 수 있습니다.

VDI의 대안

기존의 VDI는 속도가 느리고 응답하지 않는 경우도 많았을 뿐만 아니라, 원격 액세스를 지원하기 위해 데이터 센터에 서버를 대규모로 설치해야 하는 등 비용 부담이 상당했습니다. ZPA는 RDP 및 SSH를 통해 사용자를 앱에 안전한 방식으로 직접 연결시킴으로써 보다 빠르고 안전한 사용자 경험을 제공합니다. 아울러, 브라우저 또는 클라우드 브라우저 격리 기능을 통한 내장식 에이전트리스 액세스를 통해 임직원과 타사 사용자는 복잡한 데스크톱 프로비저닝 프로세스 없이 원하는 모든 장치에서 원활하게 연결할 수 있습니다.

인수합병 및 매각 지원

인수합병과 매각 건의 성공을 위해서는 업무에 반드시 필요한 주요 앱을 새로운 임직원들에게도 제공함으로써 즉시 최적의 생산성을 발휘할 수 있도록 해야 합니다. 인수합병 및 매각 과정에서 양 당사자의 IT 체계를 통합할 때, ZPA를 활용하면 그 과정을 간소화 하여 보통 수 개월이 걸리는 복잡한 작업도 단 몇 주면 완료할 수 있습니다. ZPA를 도입할 경우, VPN 없이도 업무용 앱에 원활하게 액세스할 수 있으며, 여러 네트워크를 통합하고 추가 네트워킹 장비(방화벽, 라우터, 스위치 등)을 구매할 필요가 없어 자원을 보다 중요한 업무에 투입할 수 있습니다.

OT 및 IIoT 기기를 위한 보안 액세스

임직원과 여타 공급업체는 OT 및 IIoT 자산을 정기적으로 점검하여 생산 설비의 가동 시간을 극대화하고 장비 및 공정 오류로 인한 작업 중단 사태를 방지해야 합니다. ZPA를 사용하면 현장, 공장 등 모든 곳에서 OT 및 IIoT 환경에 빠르고 안전하며 안정적으로 액세스할 수 있습니다. IoT용 ZPA는 점프 호스트 및 레거시 VPN을 사용하여 장치에 클라이언트를 설치할 필요 없이, 내부 RDP 및 SSH 대상 시스템에 완전히 격리된 클라이언트리스 원격 데스크톱 액세스가 가능합니다.

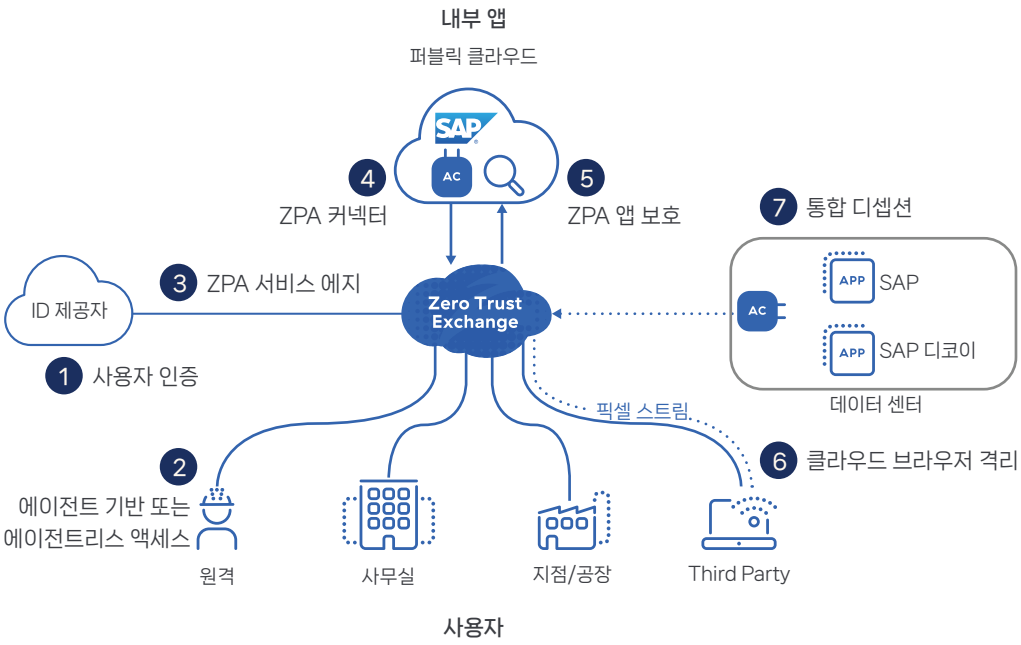
워크로드 간 연결 보안 확보

현대적인 시스템을 갖춘 기관들은 하이브리드 및 멀티 클라우드 환경에서 빠르고 안전한 워크로드 간 연결을 필요로 합니다. 워크로드용 ZPA는 클라우드 전반에 걸쳐 최소 권한 액세스 원칙 기반의 연결을 통해 가상 DMZ 및 VPN 메시의 필요성을 제거함으로써 운영 복잡성과 비용을 줄여 줍니다. 또한 워크로드는 ZPA 뒤에 숨겨져 있어, 인터넷에는 보이지 않고 공격이 불가능합니다.

Zero Trust Branch Connectivity

기존의 브랜치 및 데이터 센터 연결은 레거시 WAN, 메시 VPN, 방화벽에 의존하여 액세스를 제어하기 때문에 광범위한 공격 대상, 광범위한 권한, 라우팅 복잡성을 생성합니다. Zscaler Zero Trust Branch Connectivity는 사용자, 서버, IoT/OT 디바이스에 제로 트러스트 원칙을 적용하여 기존의 지점 내 WAN 연결 솔루션을 대체합니다.

Zscaler Zero Trust Exchange의 다이렉트 투 클라우드 아키텍처는 라우팅할 수 없는 WAN 네트워크를 통해 공격 대상과 내부 위협 이동을 제거합니다. 지점과 프라이빗 앱 간의 직접 연결을 설정하여 브랜치 커뮤니케이션을 간소화하고 애플리케이션 성능을 개선하는 동시에 ZPA에서 유연한 포워딩 및 정책 관리를 가능하게 합니다.



작동 원리

사용자(임직원, 공급사, 협력사, 도급업자)가 내부 애플리케이션에 액세스하려고 하면 ZPA는 다음을 통해 사용자를 안전하게 직접 연결합니다:

1. 기존 SAML SSO 자격 증명을 사용하여 IDP로 사용자를 인증합니다.
2. 사용자의 노트북 또는 모바일 기기에 설치된 경량 포워딩 에이전트인 Zscaler Client Connector로 사용자의 장치 상태를 확인합니다. ZPA는 또한 모든 주요 EPP/EDR/XDR 제공사(Crowdstrike, Microsoft Defender, SentinelOne 등)과의 Third Party 통합을 통해 장치 상태를 수집할 수 있습니다.
3. Zscaler 앱은 사용자의 보안 및 액세스 정책을 확인하는 브로커 역할을 하는 가장 가까운 ZPA Service Edge로 사용자의 트래픽을 전달합니다.
4. 그런 다음, ZPA Service Edge는 사용자와 가장 가까운 애플리케이션을 확인하고 서버 및 애플리케이션을 호스팅하는 환경에 설치된 경량 가상 머신인 ZPA App Connector에 대한 보안 연결을 설정합니다.
5. 두 개의 아웃바운드 터널(하나는 장치의 클라이언트 커넥터와 연결, 다른 하나는 앱 커넥터와 연결)은 ZPA 서비스 엣지를 통해 함께 연결합니다.
6. 사용자의 장치와 애플리케이션이 연결되면, 앱 커넥터는 트래픽 인라인을 자동으로 검사하여 손상되었을 가능성이 있는 사용자 또는 장치에서 비롯되는 잠재적인 위협을 감지하고 차단합니다.
7. 통합 디셉션은 디코이 앱에 액세스하는 위험 사용자를 감지하고 Zscaler Zero Trust Exchange 전체에서 내부 리소스에 대한 액세스를 차단할 수 있습니다.
8. 또한 Third Party 사용자는 통합 브라우저 기반 액세스 또는 관리되지 않는 장치에 대한 에이전트리스 액세스를 위한 클라우드 브라우저 격리를 통해 업무용 애플리케이션에 연결할 수 있습니다.

ZPA Service Edge는 클라우드(ZPA Public Service Edge)에서 Zscaler에 의해 호스팅 되거나 고객의 인프라 내에서 온프레미스 형태로 실행될 수 있습니다(ZPA Private Edge). 두 경우 모두 별도의 기기 없이 Zscaler에 의해 관리됩니다.

핵심 기능

리스크 기반 정책 엔진	인증된 유효 사용자만 프라이빗 애플리케이션에 액세스할 수 있도록 하는 강력한 네이티브 정책 엔진을 활용해 각 사용자, 디바이스, 콘텐츠 및 애플리케이션의 위험 상태를 기반으로 액세스 정책을 지속적으로 검증합니다.
통합 클라이언트 및 클라이언트리스 액세스	하이브리드 환경을 위한 최적의 보호 방안을 선택할 수 있습니다. 클라이언트 기반 액세스는 관리되는 사용자가 경량 에이전트인 Zscaler Client Connector를 통해 회사 네트워크 외부에 있는 경우에도 보호될 수 있도록 보장합니다. 클라이언트리스 액세스는 관리되지 않는 사용자에게 모든 장치와 웹 브라우저에서 원활한 앱 액세스를 제공합니다.
브라우저 액세스	BYOD 및 써드파티 사용자가 자신의 장치를 자유롭게 사용하여 클라이언트 없이도 모든 웹 브라우저를 활용하여 내부 앱에 원활하고 안전하게 액세스할 수 있습니다.
캠퍼스 ZTNA	캠퍼스 내 사용자를 위한 ZTNA를 경험함으로써 사용자는 사무실의 애플리케이션에 안전하게 접속합니다. 범용 ZTNA는 사용자와 애플리케이션의 위치에 관계없이 사용자에게 일관된 액세스 및 정책을 보장합니다.
재해 복구	고객이 제어하는 비즈니스 연속성 솔루션으로 블랙 스완 이벤트(극단적으로 예외적인 상황) 발생 시에도 미션 크리티컬 애플리케이션에 중단없이 액세스할 수 있으며, ZPA Private Service Edge를 통해 중요 프라이빗 애플리케이션에 대한 액세스 경로를 생성합니다.
앱 검색	특정 도메인의 이름과 IP 서브넷을 사용하여 애플리케이션을 자동으로 검색하고 목록을 작성하여 프라이빗 애플리케이션 자산과 잠재적으로 공격 대상이 될 수 있는 요소에 대한 세부적인 정보를 획득합니다.
AI 기반 앱 세그멘테이션	ZPA에서 자동으로 제공되는 ML 기반 세그멘테이션 관련 권장 사항을 적용하면 빠르고 쉽게 올바른 애플리케이션 세그먼트를 식별하고 적절한 액세스 정책을 수립할 수 있습니다. 수백만 개의 고객 신호와 고유한 애플리케이션 액세스 패턴에 대해 지속적으로 학습된 머신 러닝 모델을 기반으로 하는 ML 기반 세그멘테이션은 내부 공격 대상 최소화를 돕습니다.
사용자-앱 세그먼테이션	사용자별 앱 세그멘테이션을 통해 모든 애플리케이션 액세스가 '알아야 할 필요성'이 가장 낮은 권한에 따라 부여되도록 합니다. 네트워크에 사용자를 배치하지 않고도 인증된 사용자에게 특정 애플리케이션에 대한 보안 액세스를 제공할 수 있습니다. 내부 방화벽을 사용한 복잡한 네트워크 세그멘테이션이 필요하지 않습니다.
사용자-장치 세그멘테이션	사용자-장치 세그멘테이션을 통해 OT/IIoT 장비 및 시스템에 대한 모든 액세스 권한이 최소 권한 기준으로 부여되도록 합니다. 써드파티 공급업체와 원격 사용자는 IoT 및 OT용 ZPA를 사용하여 어느 위치에서나 장비에 연결할 수 있습니다.
워크로드 간 세그먼테이션	워크로드용 ZPA를 사용하면 하이브리드 및 멀티 클라우드 환경에서 워크로드 간 연결 및 통신을 보호할 수 있습니다.
앱 보호	OWASP가 밝힌 10대 공격 기법에 대한 대응책과 제로-데이 취약점을 보완할 수 있는 가상 패치를 위한 완전 맞춤형 서명을 지원하는 등 가장 널리 사용되는 'Layer 7' 웹 공격에 대한 자동 보호 기능으로 위험 사용자 및 내부 위협을 차단합니다. 모든 비공개 앱 트래픽에 대한 인라인 검사는 의심스러운 사용자 및 애플리케이션 동작을 실시간으로 모니터링합니다.
통합 디셉션	Zero Trust Exchange 전반에 걸쳐 손상된 사용자를 자동으로 격리하는 등 기본 앱 디셉션을 사용하여 가장 치밀한 공격자와 내부 위협을 탐지하고 차단합니다.
통합 클라우드 브라우저 격리	BYOD를 사용하는 계약업체와 직원에게 중요한 웹 애플리케이션에 대한 클라이언트리스 에어 갭 액세스를 제공합니다. 취약점이나 맬웨어에 감염된 관리되지 않는 엔드포인트가 네트워크나 애플리케이션을 손상시키지 않도록 합니다. 데이터 유출 제어(클립보드, 인쇄, 업로드/다운로드)를 시행하여 중요한 데이터 손실을 방지합니다.
권한 있는 원격 액세스	권한 있는 관리자와 운영자가 VPN, VDI 또는 원격 데스크톱 클라이언트(예: RDP, SSH, VNC)를 사용하지 않고도 인트라넷 웹 사이트, 내부 시스템 및 장비에 안전하게 연결할 수 있습니다.
위협 및 데이터 보호	전체 콘텐츠 검사로 위협의 위험을 줄입니다. 사용자-앱 연결 전반에서 중요한 데이터를 찾고 제어합니다.
제로 트러스트 SD-WAN	라우팅 가능한 네트워크를 노출하는 지점 및 데이터 센터의 방화벽, VPN과 같은 기존 WAN 연결 솔루션을 사용자, 서버, IoT/OT 장치를 위한 제로 트러스트 연결 솔루션으로 대체합니다.

특장점

공격 대상 최소화

취약한 VPN을 제거하고 앱을 인터넷에 노출시키지 않음으로써 권한이 없는 사용자가 앱을 찾아 공격할 수 있는 가능성을 원천 봉쇄합니다.

ZPA는 승인된 사용자와 특정 업무용 앱 사이에 하나의 보안 세그먼트를 생성하여, 모든 인바운드 연결을 제거하고 이중 암호화된 마이크로 터널을 활용해 사용자 장치에 대한 내부 연결만 허용합니다. 관련 팀들은 애플리케이션 검색 기능을 사용하여 악성 애플리케이션, 서비스 및 워크로드를 자동으로 식별하고 격리시켜 공격 대상을 더욱 줄일 수 있습니다.

위협 내부 전파 방지

연결은 최소 권한 액세스 원칙을 기반으로 하여, 네트워크에 대한 전체 액세스가 아닌 승인된 사용자가 지정한 애플리케이션을 대상으로 일대일 애플리케이션 액세스가 부여됩니다. 따라서 앱 간 이동 또는 네트워크를 통한 내부 이동은 불가능합니다. ZPA는 IP 주소를 기반으로 하지 않기 때문에 복잡한 네트워크 분할, 네트워크 접근 제어(ACL), 방화벽 정책 또는 네트워크 주소 변환을 별도로 설정하고 관리할 필요가 없습니다. 더불어, 보안 담당팀은 통합 디셉션을 활용해 조직 전체를 횡으로 가로질러 이동하려는 고도의 기술을 구사하는 공격자를 탐지하고 차단할 수 있습니다.

위험 사용자, 내부 위협 및 지능형 공격자 차단

인라인 검사, 디셉션 및 위협 격리 기능이 통합된 업계 최초의 업무용 앱 보호 기능은 다음을 통해 위험 사용자와 활성 상태인 공격자로 인한 위험을 최소화합니다:

- OWASP가 밝힌 10대 공격 기법에 대한 대응책과 제로-데이 취약점을 보완할 수 있는 가상 패치를 위한 완전 맞춤형 서명을 지원하는 등 방안을 활용해 웹 공격을 자동으로 차단
- 통합 Cloud Browser Isolation을 사용하여 관리되지 않는 장치로부터 주요 데이터를 보호하기 위해 애플리케이션에 완전히 격리된 액세스로 Third Party 및 BYOD 위험을 최소화
- 통합 디셉션에 의해 생성된 디코이 앱을 활용하고 보안 담당팀이 위험 사용자가 리소스에 접근하는 것을 차단하여 네트워크 내 위협을 억제

탁월한 사용자 경험 제공

VPN 클라이언트에 일정하고 빠른 속도로 연결(로그인 및 로그아웃할 필요 없음)할 수 있는 역량을 확보함으로써 원격 사용자에게 더 빠르고 안전한 액세스 경험을 보장합니다. Third Party 도급업자, 공급사, 협력사 등은 별도의 클라이언트를 설치할 필요 없이 모든 장치 및 웹 브라우저에서 원활한 액세스를 누릴 수 있습니다. 사용자 등록은 Azure AD, Okta, Ping 등과 같은 기존 SSO 로그인 자격 증명으로 가능합니다. 아울러, 관리자는 업무용 앱의 액세스 문제, 네트워크 경로 중단 또는 네트워크 정체 현상으로 인한 최종 사용자 성능 문제를 사전에 감지하고 해결함으로써 사용자의 생산성을 높게 유지할 수 있습니다.

앱, 워크로드 및 장치 전반에 걸친 보안 액세스를 위한 통합 플랫폼

업무용 앱, 워크로드 및 OT/IIoT 장치 전반에 걸쳐 제로 트러스트를 확장하여 각각 분리되어 있는 여러 개의 원격 액세스 도구를 간소화 및 통합하고 보안 및 액세스 정책을 통합함으로써 공격을 막고 운영 복잡성을 줄일 수 있습니다.

사용자 에디션용 ZPA

	ZPA Essentials Edition	ZPA Business Edition	ZPA Transformation Edition	ZPA Unlimited Edition
Platform services	Source IP Anchoring, Multiple IdP, LSS	(+) Extended DC Access	(+) Test Environment, Customer PKI	(+) Test Environment, Customer PKI
User-to-app segmentation	10 App Segments	500 App Segments	Unlimited App Segments	Unlimited App Segments
App Connector	20 Pairs	50 Pairs	Unlimited Pairs	Unlimited Pairs
On-campus ZTNA[1]	1 Pair (Virtual)	1 pair Private Service Edge per 5,000 users	1 Pair Private Service Edge per 2,000 users	1st Private Service Edge Pair included, add'l Pair for every 1,000 users
Clientless Access[2]	—	✓	✓	✓
Integrated digital experience monitoring	—	Standard	Standard	Standard
Dynamic Risk-based Policy	—	Standard	Advanced	Advanced Plus
AppProtection	—	—	✓	✓
Integrated isolation	—	—	Standard	Advanced Plus
Data protection (private apps)	—	—	—	✓
Premium support	—	—	—	✓

핵심 차별화 요소

업계 유일의 차세대 ZTNA 플랫폼인 Zscaler Private Access는 타의 추종을 불허하는 사용자 경험으로 탁월한 보안 역량을 제공합니다.

- **처음부터 최소 권한 액세스를 고려한 설계:** 승인된 사용자가 네트워크가 아닌 승인된 리소스에만 연결할 수 있도록 허용(레거시 VPN으로는 불가능한 기능)합니다.
- **앱을 공격자에 노출시키지 않아 공격을 원천 봉쇄:** 업무용 앱, 워크로드 및 장치를 퍼블릭 인터넷에 보이지 않게끔 하여, 앱 손상, 데이터 도난 및 내부 이동을 차단합니다.
- **전체 인라인 검사:** 가장 널리 사용되는 유형의 웹 공격을 자동으로 방지하여 업무용 앱의 악용을 식별하고 차단합니다.
- **통합 디셉션:** 네이티브 앱 디셉션 기능이 있는 유일한 ZTNA 솔루션으로 위협 내부 전파 시도 및 랜섬웨어의 확산을 방지합니다.
- **광범위한 글로벌 에지 보급:** 전 세계 150여 개의 클라우드 엣지를 통해 탁월한 보안 및 사용자 경험을 보장할 수 있습니다. 또한, 옵션으로 선택 가능한 로컬 서비스 에지는 제로 트러스트를 HQ로 확장합니다.

[1]ZPA Business 에디션은 최대 5개의 프라이빗 서비스 에지 페어를 지원하며, 사용자가 50,000명을 초과하면 추가 페어를 구매해야 합니다. ZPA Transformation 에디션은 최대 10개의 프라이빗 서비스 에지 페어를 지원하며, 사용자가 50,000명을 초과하면 추가 페어를 구매해야 합니다. ZPA Unlimited 에디션은 최대 50개의 프라이빗 서비스 에지 페어를 지원하며, 사용자가 50,000명을 초과하면 추가 페어를 구매해야 합니다.

[2]Clientless Access에는 브라우저 액세스 및 권한 있는 원격 액세스 (최대 10개 시스템용)가 포함됩니다.

- **클라우드 네이티브 기반:** 조직이 성장함에 따라 필요한 기능을 값비싼 온프레미스 기기나 복잡한 인프라를 도입할 필요 없이 클라우드 기반 플랫폼의 확장성을 활용하여 확보할 수 있습니다.
- **각종 사용자, 워크로드 및 장치를 위한 통합 ZTNA 플랫폼:** 업계에서 가장 커버리지가 넓은 ZTNA 플랫폼으로 업무용 앱, 서비스 및 OT 장치에 안전하게 연결합니다.
- **확장 가능한 제로 트러스트 플랫폼과 호환:** 완벽한 보안 서비스 에지(SSE) 프레임워크를 기반으로 구축된 Zero Trust Exchange를 활용해 조직을 보호하고 강화합니다.

기본 구성 요소

Zscaler Client Connector

Client Connector는 사용자의 노트북 및 모바일 기기에서 실행되는 경량 애플리케이션으로 사용자 트래픽을 가장 가까운 Zscaler Service Edge로 자동 전달함으로써 모든 장치, 위치 및 애플리케이션에 걸쳐 보안 및 액세스 정책이 구현되도록 지원합니다.

Gartner

가트너 SSE MQ에서 리더로 선정된 Zscaler, 실행역량 부문 최고 등급 부여

Zscaler Branch Connector

Branch Connector는 지점 또는 데이터 센터에서 실행되는 가상 머신으로, 모든 리소스에서 가장 가까운 Zscaler Service Edge로 트래픽을 전달합니다. Zscaler Zero Trust Exchange를 통해 모든 네트워크에서 Client Connector를 설치할 수 없는 사용자, 서버, IoT/OT 장치와 애플리케이션 간의 양방향 통신을 가능하게 합니다.

Zscaler Clientless Access

사용자는 통합 브라우저 기반 액세스(웹, RDP, 또는 SSH)를 통해 업무용 앱, 워크로드 및 IIoT/OT 장치에 안전하게 연결할 수 있으며, 관리되지 않는 장치에서 클라이언트리스 액세스를 위한 Cloud Browser Isolation을 사용할 수 있습니다.

ZPA App Connector

App Connector는 데이터 센터 또는 퍼블릭 클라우드에 배포된 업무용 애플리케이션 전방에 배치되는 경량 가상 머신으로, 앱을 인터넷에 노출하지 않는 내부 연결을 통해 승인된 사용자와 지정된 앱 간의 보안 연결을 중개합니다.

ZPA Service Edges

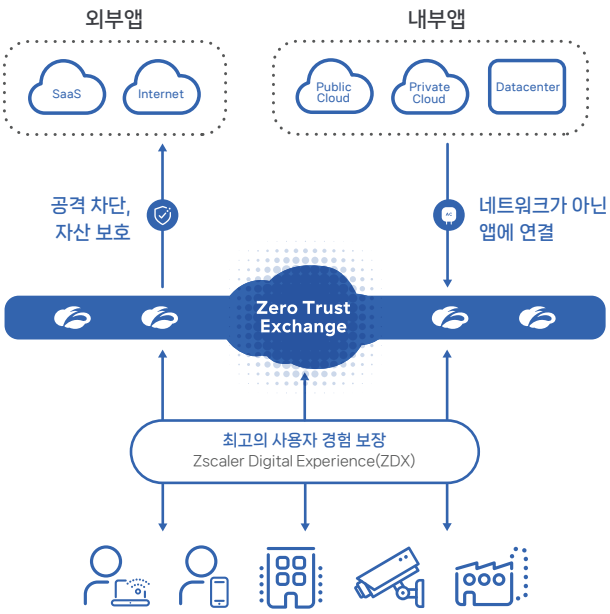
Service Edge는 권한이 승인된 사용자(Client Connector 및 Browser Access 사용)과 특정 업무용 애플리케이션(App Connector 사용) 간의 내외부 연결을 결합하여 보안 및 액세스 정책을 구현합니다.
대부분의 고객은 전 세계 150여 개의 거래소에서 호스팅 되고 세계 최대 규모의 조직에서 수백만 명의 사용자를 동시에 처리할 수 있는 Public Server Edge를 활용합니다. Zscaler에서 관리하는 Private Service Edge의 경우, 온프레미스 사용자에게 로컬 네트워크를 벗어나지 않고도 온프레미스 애플리케이션을 최단 경로로 액세스할 수 있는 방안을 제공하기 위해 고객의 사업장에서 호스팅할 수도 있습니다.

Zero Trust Exchange 호환 플랫폼 ZPA

The Zscaler Zero Trust Exchange™는 사용자, 워크로드, 장치를 기업 네트워크에 두지 않고도 연결할 수 있는 완벽한 보안 서비스 에지(SSE)를 지원하는 클라우드 네이티브 플랫폼입니다. 네트워크를 확장하고, 공격 대상을 확장하며, 내부 위협 이동의 위험을 높이고, 데이터 손실을 방지하지 못하는 경계 기반 보안 솔루션과 관련된 보안 위험과 복잡성을 줄여줍니다.

Zscaler가 사용자, 워크로드 및 IIoT/OT를 대상으로 제로 트러스트를 구현하는 방법

단 몇 주면 배포를 완료하여, 사이버 보안 및 사용자 경험을 향상



모든 사용자, 모든 장치, 모든 앱, 모든 위치

기술 사양

Zscaler 구성 요소	지원 플랫폼 및 시스템
Client Connector	iOS 9 or later / macOSX 10.10 or later / Android 5 or later / CentOS 8 / Windows 7 or later / Ubuntu 20.04
Branch Connector	Centos, Redhat / VMware vCenter or vSphere Hypervisor
Clientless Access	Modern web browsers(HTML 5-capable): Chrome / Edge / FireFox
App Connector	AWS / Microsoft Hyper-V / Centos, Oracle, Redhat / VMware vCenter or vSphere Hypervisor / Microsoft Azure

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