citrix

솔루션 브리핑

Citrix Secure Private Access를 통한 제로 트러스트 네트워크 액세스

디지털 트랜스포메이션, 클라우드 도입 및 하이브리드 인력의 확장은 보안 및 연결 환경의 역학관계를 근본적으로 바꾸어 놓았습니다. 그 결과, 기업들은 애플리케이션에 의존하고 있으며, 그 어느 때보다 많은 직원들이 인터넷과 다양한 유형의 기기(관리형 및 비관리형)를 사용하여 교류하고 있습니다.

이러한 변화에 따라, 사이버 보안 전문가들은 업무 연속성과 훌륭한 직원 경험을 보장하면서도 보안을 유지하고 확장하기 위해 노력해 왔습니다. 이와 동시에, 더 많은 애플리케이션이 클라우드로 이동하면서 더 많은 워크로드가 퍼블릭 클라우드와 SaaS에 분산되었습니다. 그 결과, 앱 환경이 변화하고 있으며 더욱 복잡해지고 있습니다.

빠른 속도로 확장되는 공격 표면

기존의 엔터프라이즈 아키텍처와 사일로화된 접근 방식은 주로 데이터센터 보안, 포인트 제품 및 기업 또는 지점 네트워크의 중복 방화벽에 의존했습니다. 안타깝게도, 이러한 접근 방식은 오늘날의 동적 앱 연결, 규제 준수 및 보안 요건에 맞지 않습니다. 더 많은 클라우드 마이그레이션이 진행됨에 따라, 데이터센터 또는 프라이빗 클라우드보다 퍼블릭 클라우드에 더 많은 중요 데이터와 비즈니스 크리티컬 애플리케이션이 상주하고 있습니다. 안타깝게도 이렇게 복잡한 환경은 보안을 유지하고 관리하기가 더욱 어려워지고 있으며, 오늘날 IT 팀이 직면하고 있는 복잡성을 처리하는 데 필요한 전문 지식 차원에서 볼 때 특히 그러합니다.

하이브리드 업무 모델이 성장하고 다양한 유형의 기기 사용이 늘어남에 따라 공격 가능한 조직의 표면도 확장된 셈입니다. 기업에서 관리하는 기기는 IT 부서가 가장 많은 통제력을 가지고 있기 때문에 원격 액세스를 제공하는 가장 안전한 방법인 경우가 많지만 직원이나 계약업체는 BYO (Bring Your Own) 기기를 사용해야 하거나 이를 선호할 수 있기 때문에 보안 이벤트의 위험이 높아집니다.

이러한 모든 복잡성과 확장된 공격 표면은 공격자에게 기회를 제공합니다. 그 결과, 조직들은 보안에 대한 접근 방식을 재고하는 동시에, 직원들이 최대한 원활하게 언제 어디서나 어떤 기기에서든 애플리케이션에 안전하게 액세스할 수 있도록 해야 합니다.

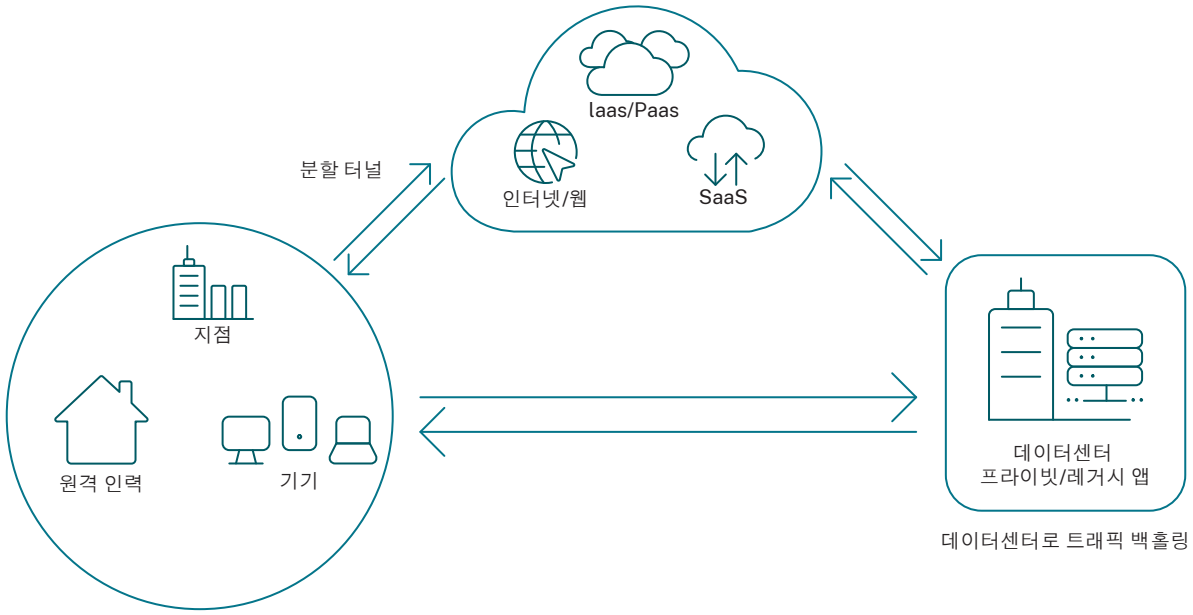


그림 1: 기존 네트워크 및 보안 방식

새로운 하이브리드 업무 모델 및 기존 접근 방식의 문제

조직이 새로운 하이브리드 업무 모델을 현대화하고 이에 적응하는 과정에서, 사용자, 데이터 및 애플리케이션을 보호하려면 우선 포괄적인 가시성과 제어가 필요합니다. 클라우드 환경으로의 전환 과정은 조직마다 다릅니다. 조직이 당면한 문제는 비즈니스 애플리케이션, 보안 및 네트워킹 기술, 연결 요건 및 해결해야 할 결함이 무엇인지에 따라 달라집니다.

포인트 제품 및 기존의 보안 및 네트워킹 접근 방식과 관련된 몇 가지 일반적인 문제는 다음과 같습니다.

- 부적절하고 일관되지 않은 보안 정책: 다중 로그인 및 중복되는 보안 정책으로 인해 안전하지 않은 관행과 보안 위험 증가를 초래할 수 있습니다.
- IT 비용 및 복잡성 증가: 여러 벤더를 관리하는 것은 비용이 많이 들고 비효율적이며 복잡합니다.
- 부수적 피해로서의 사용자 환경 저하: 최종 사용자 경험 저하, 낮은 도입률, 쉐도우 IT(Shadow IT)

Citrix Secure Private Access– 정의

Secure Private Access는 Citrix의 광범위한 Secure Access 솔루션의 일부분으로서, 오늘날의 분산된 엔터프라이즈 환경에서 발생하는 주요 문제를 해결하고 복잡성을 줄이는 데 도움을 줍니다.

Citrix Secure Private Access

Citrix Secure Private Access는 사용자 ID, 위치 또는 엔드유저 기기에 관계없이 제로 트러스트(Zero Trust) 접근 방식을 통해 상시 접속 보안을 제공하는 클라우드 제공 ZTNA 솔루션입니다. 이 솔루션은 기존 VPN 접근 방식에서 일반적으로 발생하는 트래픽 백홀을 방지하여 IT 부서에서 승인한 모든 애플리케이션에 대해 안전하고 빠른 연결을 보장하며, 무단 액세스 또는 관리되지 않는 기기 및 BYO(Bring Your Own) 기기로부터 발생하는 위협으로부터 사용자와 인프라를 보호하는 보안 클라우드 서비스로서 모든 지리적 위치에서 사용할 수 있으며 사용자 기반과 사용량이 증가함에 따라 자동으로 확장되어 민첩성을

제공하는 동시에 최상의 사용자 환경과 보안을 위해 상시 접속 보안 기능을 제공합니다. 완전 관리형 서비스이므로 IT 부서는 데이터센터 전반에 걸쳐 어플라이언스를 관리하는 데 시간을 소비하는 대신 전략적인 이니셔티브에 더욱 집중할 수 있습니다.

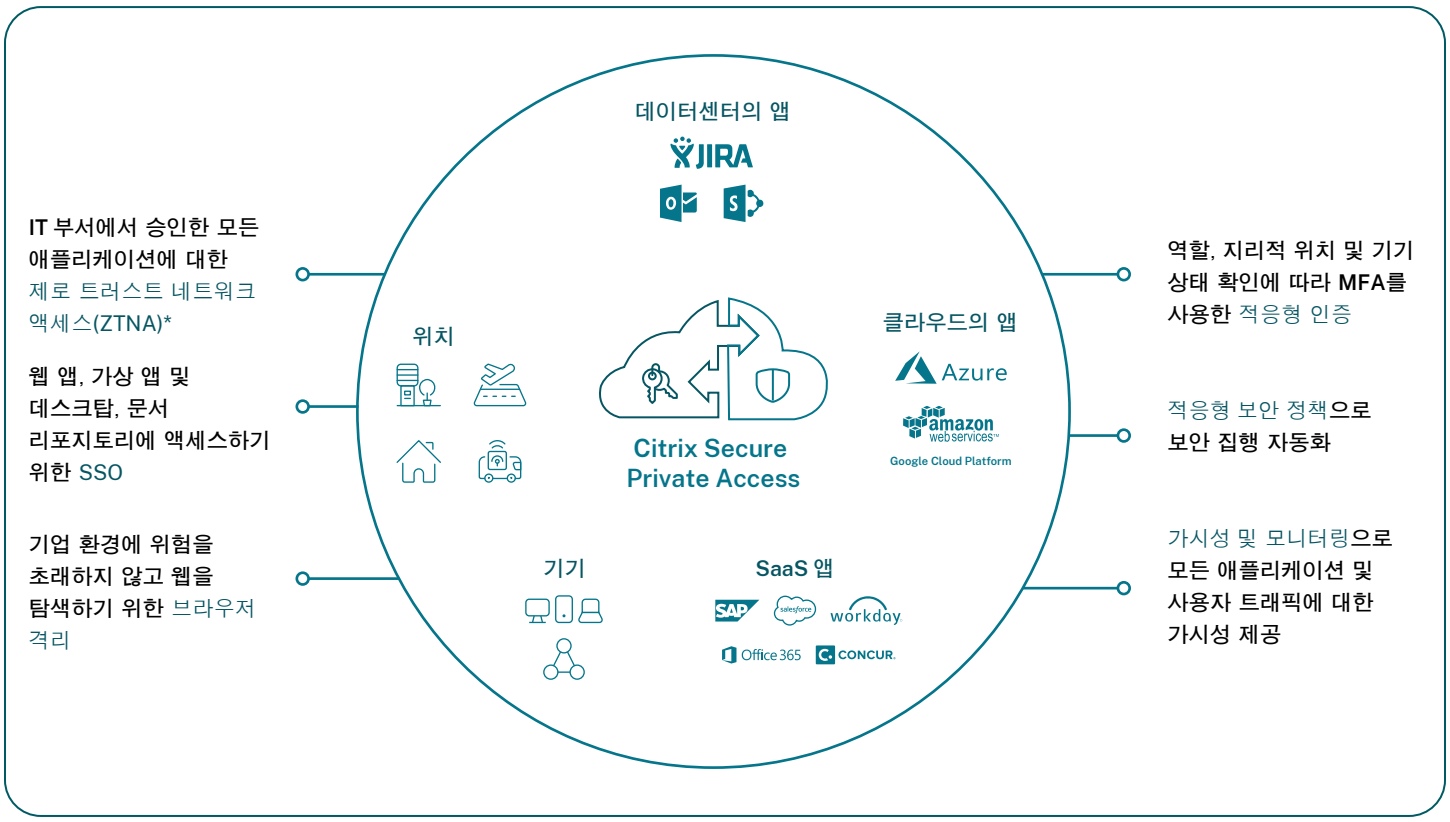
Citrix Secure Private Access를 통해 IT 부서는 직원, 계약업체 및 파트너에게 특정 애플리케이션에 대한 액세스를 제공할 뿐만 아니라 원격 근무 직원이 BYO (Bring Your Own) 기기를 사용하여 애플리케이션에 안전하게 액세스할 수 있는 방법을 제공할 수 있습니다.

적응형 액세스 정책을 기반으로, BYO (Bring Your Own) 기기의 사용자 세션을 원격 브라우저 격리 세션으로 자동 리디렉션할 수 있습니다. 이렇게 하면 BYO (Bring Your Own) 기기의 악성 콘텐츠가 애플리케이션이나 네트워크로 전송되는 일을 방지할 수 있습니다. 또한 개인 기기에 기업 정보를 다운로드하는 기능도 방지합니다. 그에 더해, Secure Private Access는 앱 보호 정책을 제공하고, 사용자의 세션뿐만 아니라 Workspace를 통해 액세스되는 민감한 정보가 모든 키로거(keylogger) 및 스크린 캡처 멀웨어로부터 보호되도록 합니다.

제로 트러스트 네트워크 액세스(ZTNA)

제로 트러스트는 기존 신뢰 보안 원칙을 거부합니다. 그 대신, 제로 트러스트는 '절대 신뢰하지 말고 항상 검증'하는 것에 집중합니다. 이전의 Castle and Moat 접근 방식을 사용하는 기존 솔루션은 로그인 시에만 사용자를 인증하고 승인하는 데 중점을 두며, 인증 시 사용자를 기본적으로 신뢰합니다. 이러한 접근 방식은 사용자의 기기 또는 자격 증명이 도난당하거나 해킹되기 쉬운 무단 액세스를 다수 발생시키고 있습니다.

제로 트러스트를 통해 조직은 세션 내내 사용자 활동을 지속적으로 모니터링 및 평가하고 감지된 이상을 기반으로 보안 제어를 자동화할 수 있습니다.



포괄적이고 통합된 제로 트러스트 보안 전략	IT 부서가 사용자, 애플리케이션, 파일 및 엔드포인트 전반에 걸쳐 포괄적인 제로 트러스트 보안 전략을 구현할 수 있도록 지원합니다.
IT 부서에서 승인한 모든 애플리케이션에 대한 제로 트러스트 네트워크 액세스(ZTNA)	VPN은 확장하기가 어렵고, 개인정보보호에 대한 우려를 일으키며, 오늘날의 최신 보안 표준을 충족하지 못합니다. Citrix Secure Private Access는 이러한 애플리케이션이 웹이든, SaaS, 클라이언트/서버 애플리케이션(TCP)이든, 아니면 가상 애플리케이션이든, 이러한 앱이 온프레미스 또는 퍼블릭 클라우드에 배포되든, 아니면 Citrix Workspace 내부 또는 외부에서 액세스되든 관계없이, IT 부서에서 승인한 모든 애플리케이션에 대한 ZTNA (Zero Trust Network Access)를 제공하여 기대하는 제로 트러스트 결과를 달성합니다.
적응형 인증, SSO 및 보안 강화	Citrix Secure Private Access는 사용자 세션이 설정되기 전과 후에 엔드 유저 기기를 스캔하는 기능을 제공합니다. 관리자는 사용자 위치 및 기기 상태 평가 결과에 따라 애플리케이션에 대한 사용자 액세스 인증 및 권한 부여 방법을 정의할 수 있습니다. 이러한 정책을 통해, 관리자는 이 애플리케이션 내에서 사용자가 수행할 수 있는 작업을 제어할 수 있습니다. 이러한 정책은 Citrix Virtual App and Desktop service 고객용을 포함한 모든 애플리케이션에 구현할 수 있습니다.
통합 원격 브라우저 격리 기술을 통해 BYO (Bring Your Own) 및 관리되지 않는 기기를 사용하여 IT 부서에서 승인한 앱에 안전하게 액세스	Citrix Secure Private Access를 통해 사용자는 엔드 유저 기기에 엔드포인트 에이전트를 설치하지 않고도 자신의 BYO (Bring Your Own) 기기에서 IT 부서가 승인한 앱에 액세스할 수 있습니다. 하지만 로컬 브라우저에서 호스팅되는 보안 브라우저 서비스로 사용자 세션을 리디렉션합니다. 이를 통해 사용자는 샌드박스 환경에서 앱에 액세스하고 생산성을 유지할 수 있습니다. 이와 동시에, 브라우저 격리 기능을 통해 인터넷의 악성 콘텐츠로부터 엔드포인트와 네트워크를 보호하여 기업 리소스로부터 에어갭을 생성합니다.
키로거 및 스크린 캡처 멀웨어로부터 보호	IT 부서는 조직에서 관리하는 기기를 면밀히 모니터링할 수는 있지만 관리되지 않는 기기의 상태에 대한 통찰력은 부족합니다. 이로 인해, 멀웨어에 감염된 기기, 특히 키로거 또는 스크린샷 멀웨어가 침투한 기기는 공격자가 민감한 기업 데이터를 유출하게 할 수 있으므로 위험을 초래합니다. Citrix Secure Private Access는 Workspace App을 통해 액세스되는 애플리케이션의 스크린샷을 키로거(keylogger) 및 스크린 캡처 멀웨어로 캡처하거나 사용자 자격 증명을 훔치는 일을 방지하는 제어를 집행합니다.

모든 애플리케이션 및 사용자에 대한 엔드투엔드 가시성	Citrix Secure Private Access는 IT 부서에서 승인한 모든 애플리케이션에 대한 모든 사용자 트래픽에 대해 완전한 엔드투엔드 모니터링 및 가시성을 제공합니다. 모든 사용자 트래픽을 모니터링하기 위해 여러 대시보드가 포함된 다중 액세스 솔루션을 보유한 고객은 모니터링을 간소화하고 사일로형 환경을 통합하는 단일 대시보드의 장점을 이용할 수 있습니다.
잠재적 위험 감지 및 방어	Citrix Analytics for Security는 애플리케이션, 기기 및 네트워크에 대한 통찰력을 제공하여, 사용자 행동 및 시스템에서 감지된 이상에 따라 보안 시행을 자동화하는 데 도움을 줍니다. 이를 통해 IT 부서의 수작업을 줄이고, 시기적절한 집행을 가능하게 하며, 무단 침해의 위험을 줄일 수 있습니다.

요약

애플리케이션 및 데이터 보안 액세스 측면에서 위협 및 취약성으로부터 보호하는 것 이상으로 고려할 점이 많습니다. 직원들의 생산성과 참여를 유지할 수 있도록, 여러 번 로그인하거나 패스워드를 계속 번거롭게 재설정하지 않고 액세스할 수 있어야 합니다.

그렇기 때문에 Citrix Secure Private Access 솔루션은 다음 두 가지 분야, 즉 어디서나 원활하게 일할 수 있는 애플리케이션 경험과 첨단 적응형 및 클라우드 제공 보안의 장점을 제공하도록 설계되어 있습니다. 기존 온프레미스 VPN과 달리 엔드투엔드 제로 트러스트 보안은 사용자가 전체 네트워크에 액세스할 필요 없이 IT 부서에서 승인한 모든 애플리케이션에 원격으로 액세스할 수 있도록 합니다. 이 제로 트러스트 접근 방식을 사용하면 신원, 지리적 위치 및 기기 상태와 같은 컨텍스트의 조합을 사용하여 애플리케이션이 사용되는 위치와 방법에 따라 액세스 권한을 부여할 수 있습니다.

한편, 전체 클라우드 제공 보안 스택은 더 많은 직원들이 재택 근무를 하고 있기 때문에 특히 중요합니다. 전체 커버리지 및 복원력을 위해 설계된 글로벌 클라우드 서비스 솔루션을 사용할 경우, 정책 및 보호 조치가 현재 위협 환경에 맞게 자동으로 업데이트됩니다.

https://www.citrix.com/products/citrix-secure-private-access/에서 Citrix Secure Private Access에 대해 자세히 알아보십시오.

citrix

기업 영업
북미 | 800-424-8749
전 세계 | +1 408-790-8000

위치
기업 본사 | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States