ivanti

Ivanti Neurons for Zero Trust Access

제로 트러스트, 번거로움 제로: 쉽게 Everywhere Work를 경험해보세요

Ivanti Neurons for ZTA는 조직이 국경 없는 디지털세상에서 Everywhere Work를 도입할 수 있도록 지원 합니다. ZTA는 지속적인 인증 및 적응형 제어를 통해 애플리케이션 중심의 안전한 접속을 제공합니다.

ZTA는 Identity와 컨텍스트를 우선시함으로써 공격 표면을 최소화하고, 측면 이동 위협을 방지하며, On-premise, public 및 private cloud 등 배포된 애플리케이션 에코시스템 전반 의 가시성을 향상시킵니다. 자동화된 위협 탐지, 세분화된 정책 적용, 유연한 게이트웨이 배포 옵션을 제공하는 ZTA는 제로 트러스트 원칙을 자신 있게 채택하고 사용자, 애플리케이션, 데이터를 보호하고자 하는 조직에 적합한 솔루션 입니다.

어디서나 제로 트러스트 액세스

오늘날의 국경 없는 디지털 환경에서 조직은 원격근무의 증가와 클라우드 기반 애플리케이션 및 서비스의 채택 증가로 인해 복잡한 보안 문제에 직면해 있습니다. 직원들의 재택근무 '혁명'으로 기존의 네트워크 경계가 확장되면서 거의 모든 곳에서 기업 리소스에 액세스 해야 하는 분산되고 동적인 인력이 생겨났습니다.

이러한 변화로 유연성과 효율성이 향상되었지만 새로운 취약점과 노출지점이 생겼습니다. 기업은 AI를 활용한 공격을 비롯하여 고도화되고 정교한 공격 등 빠르게 진화하는 위협 환경에 대응해야 합니다. 따라서 기존의 보안 접근 방식은 더 이상 적절하지 않으며, 기업은 애플리케이션과 데이터에 대한 액세스를 보호하는 방법을 재평가해야 합니다.

최신 보안 문제를 해결하고 조직이 제로 트러스트 네트워크 접속 원칙을 자신 있게 수용할 수 있도록 설계된 종합 Ivanti Neurons for ZTA을 소개합니다. 지속적인 검증, 세분화된 정책 시행, 실시간 위험 평가에 중점을 둔 Ivanti Neurons for ZTA은 강력하고 탄력적인 보안 및 접속 관리 전략의 토대를 제공합니다.

Everywhere Work를 위한 안전한 액세스

조직이 제로 트러스트 원칙을 준수하고 Everywhere Work 모델을 지원할 수 있도록 하세요. On-premise, 데이터 센터, public 및 private cloud 등 다양한 환경에서 사용자, 애플리케이션, 디바이스 및 컨텍스트를 지속적으로 인증하고 기업 애플리케이션에 대한 액세스를 보호합니다.

애플리케이션 중심 액세스로 보안 강화

제로 트러스트 네트워크 액세스(ZTNA)로 보안 태세를 강화하고 측면 이동 공격으로부터 보호하세요. ZTNA를 사용하면 최소 권한 원칙에 따라 액세스 권한을 부여하여 애플리케이션이나 콘텐츠에 액세스해야 하는 사용자만 연결되도록 할 수 있습니다. 또한, ZTNA를 사용하면 애플리케이션 중심의 액세스를 제공하여 보안을 강화하는 동시에 사용자 신원과 디바이스 보안 상태를 지속적으로 확인할 수 있습니다.

적응형 애플리케이션 정책 및 제어

사용자 ID, 디바이스, 위치 등을 기반으로 애플리케이션 액세스를 세밀하게 제어할 수 있습니다. 계약자 액세스 관리 또는 위치 기반 인증 시행 등 조직의 비즈니스 요구 사항에 맞게 액세스 정책을 조정하세요.

사용자 및 엔티티 행동 분석(UEBA)을 통한 선제적 위협 탐지

UEBA 및 고급 위험 분석을 활용하여 이상 징후를 식별하고 위험을 평가하며 잠재적 위협에 실시간으로 대응하세요. 취약성에 대한 가시성을 제공하고 관리자가 효율적으로 위험을 분류할 수 있도록 Ivanti Neurons for VULN KB의 취약성 위험 등급(VRR) 점수를 활용하여 엔드포인트 애플리케이션을 평가할 수 있습니다.

액세스 관리 간소화

사용자 또는 그룹에 필요한 애플리케이션에 대한 액세스 권한을 신속하게 부여하여 강력한 보안을 유지하면서 비즈니스 운영을 원활하게 하세요. M&A시 액세스 관리를 간소화하고 새로운 사업부를 원활하게 통합할 수 있습니다.

클라우드 접속 보안 브로커(CASB) 및 보안 웹 게이트웨이(SWG)와의 통합

ZTA와 CASB 및 SWG 기능을 통합하여 보안 액세스 전략을 강화하세요. 데이터 손실 방지(DLP), 엔터프라이즈 디지털 권한 관리(EDRM), 광학 문자 인식(OCR), 멀웨어 탐지 등의 기능으로 SaaS 및 인터넷 애플리케이션에 대한 안전한 액세스를 보장하세요.

작동 방식

클라우드 호스팅 인증 및 권한 부여

ZTA는 애플리케이션 세션을 설정하기 전에 클라우드 호스팅 컨트롤러를 사용하여 사용자 신원 및 기기 보안 상태를 인증하고 권한을 부여하여 규정을 준수하도록 합니다.

중앙 집중 정책 엔진 및 UEBA

ZTA는 중앙에서 관리되는 정책 엔진을 통해 모든 접속 요청과 세션을 제어하고, 사용자 및 엔티티 행동분석(UEBA)으로 추가적으로 보안을 제공합니다. 각 세션의 속성을 모니터링하고 평가하며, 독자적인 위험 점수를 통해 규정 미준수, 악의적, 비정상적인 활동을 식별하여 신속하게 위협을 완화합니다.

유연한 게이트웨이 배포

ZTA gateway는 on-premise 또는 public or private cloud 환경 중 원하는 곳에 배포할 수 있습니다. 클라우드 애플리케이션과의 근접성은 사용자 경험을 최적화하고, 지연 시간을 줄이며, 확장 가능한 하이브리드 IT 배포를 가능하게 합니다.

애플리케이션별 다이렉트 보안 터널 제공

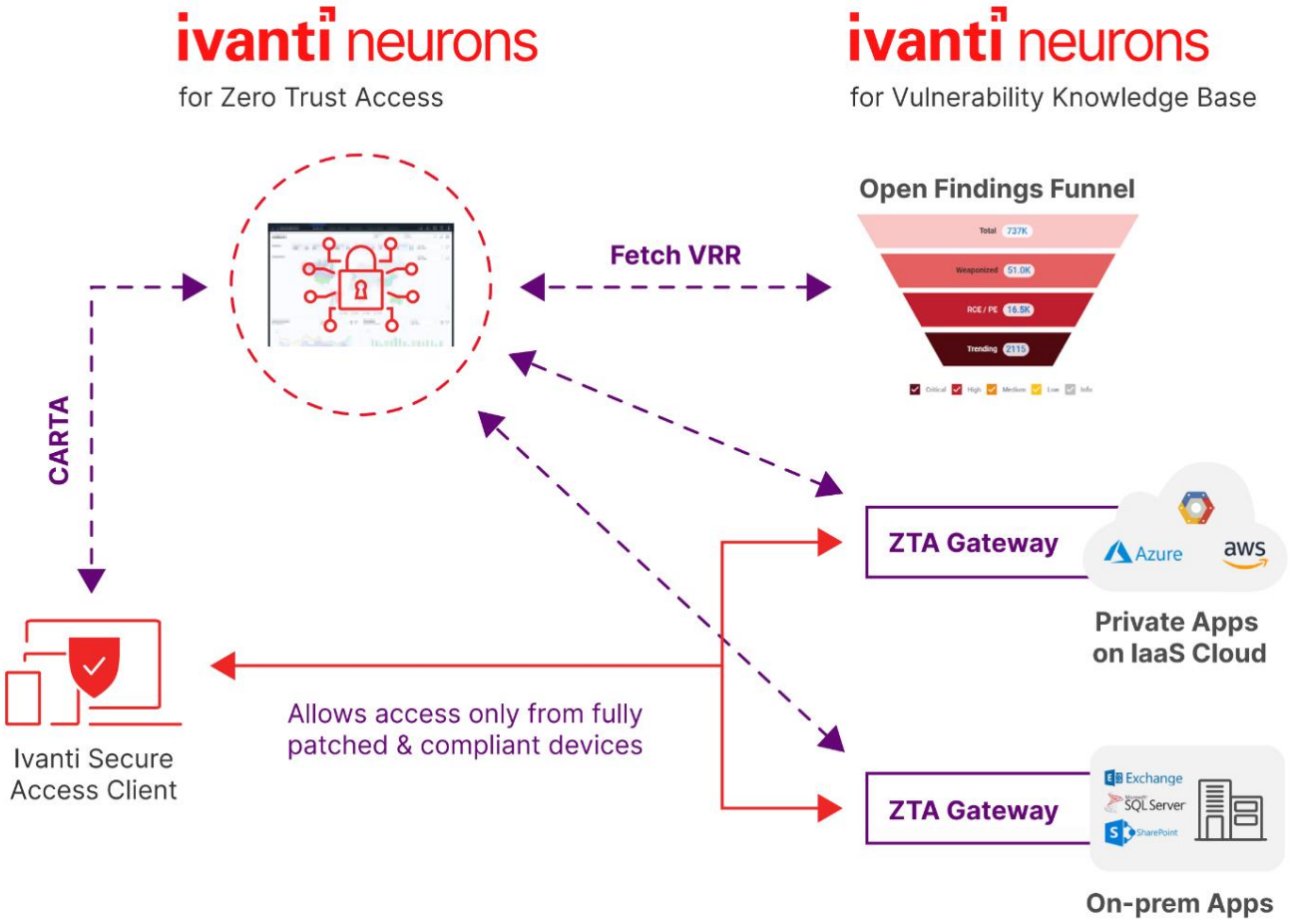
ZTA 컨트롤러는 애플리케이션 접근 정책을 검증하고 Ivanti Unified Client에 지시하여 장치와 ZTA Gateway 간에 직접적이고 보안된 애플리케이션별 mTLS 터널을 생성합니다. ZTA 컨트롤러와의 데이터 상호 작용은 제거됩니다.

지능형 트래픽 조정

Ivanti Unified Client는 애플리케이션 터널을 연결하기 위해 가장 최적의 게이트웨이로 트래픽을 자동으로 유도하여, 비용이 많이 드는 백홀링(backhauling)이나 헤어핀(hair-pinning) 트래픽의 필요성을 제거합니다.

실시간 위험 평가

ZTA는 사용자 행동, 디바이스 보안 상태, 취약성 위험 등급(VRR) 점수를 기반으로 위험 수준을 지속적으로 평가하여 선제적인 위협 완화를 가능하게 합니다. 기존 VPN과의 원활한 통합: ZTA는 기존 VPN 솔루션과 통합되어 강력한 보안을 유지하면서 새로운 앱에 안전하게 액세스하고 비즈니스 활동을 지원할 수 있습니다.



Ivanti Neurons for ZTA가 해결하는 주요 사용 사례를 살펴 보겠습니다:

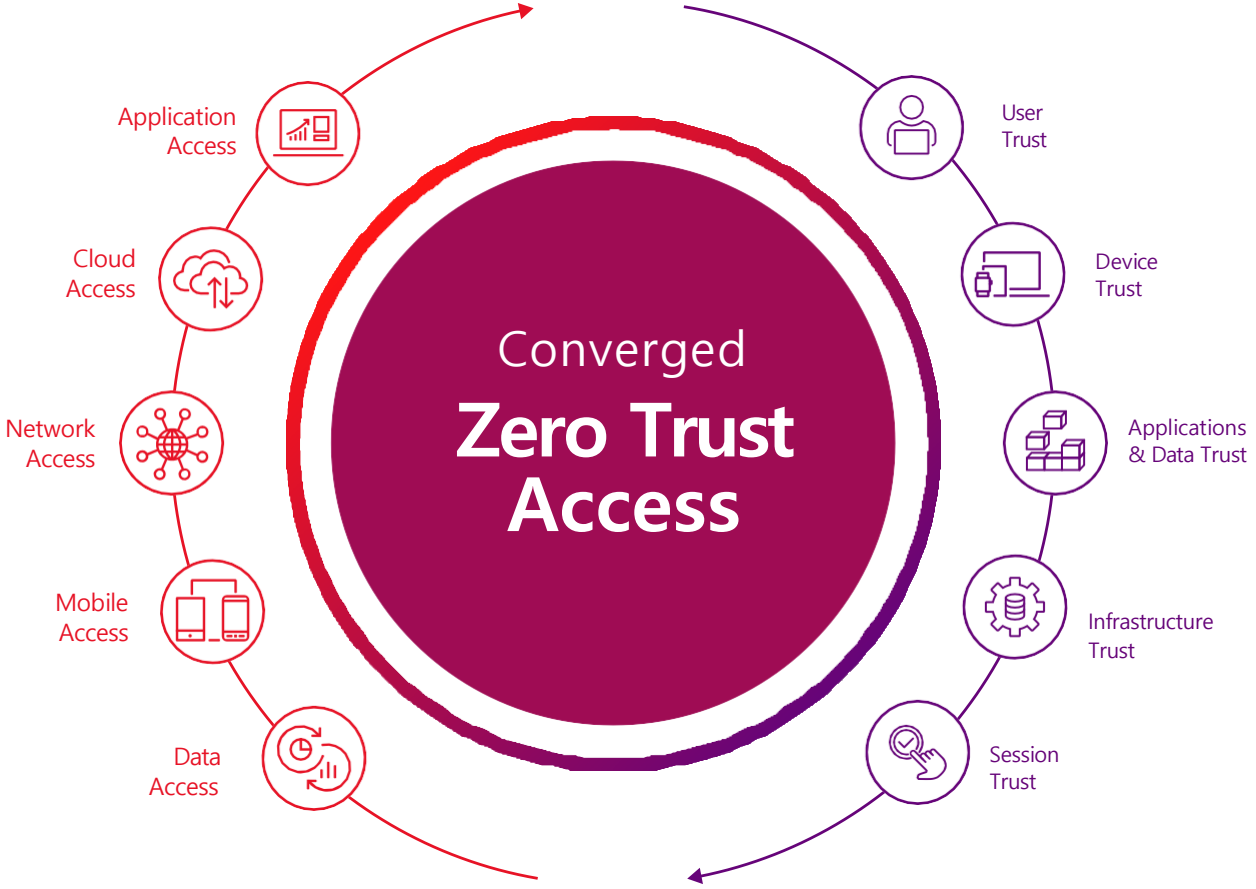
재로 트러스트 액세스 모델 구현

조직이 점점 더 경계가 없는 네트워크 환경을 탐색하고 Everywhere Work로 전환함에 따라 제로 트러스트 액세스 모델을 구현하는 것은 보안을 강화하는 데 필수적입니다. Ivanti Neurons for ZTA는 애플리케이션 중심 접근 방식을 채택하여 광범위한 네트워크가 아닌 애플리케이션에 대한 액세스를 보호하는 데 중점을 둔 강력한 솔루션을 제공합니다. 최소 권한 원칙을 적용하여 사용자에게 권한이 부여된 특정 애플리케이션만 액세스 권한을 부여합니다. 사용자 신원을 지속적으로 확인하고 디바이스 보안 상태를 평가하여 보안 조치를 강화합니다. 또한 이 솔루션은 Ivanti Connect Secure VPN과 Ivanti Neurons for ZTA 모두 원활하게 지원하는 통합 클라이언트를 제공하여 세분화된 접속 제어로 측면 이동 공격으로 부터 선제적으로 보호할 수 있습니다.

애플리케이션 액세스 제어 및 관리

애플리케이션 액세스의 제어 및 관리는 조직의 데이터와 리소스를 보호하는데 중요한 역할을 합니다. Ivanti Neurons for ZTA를 사용하면 사용자 ID, 디바이스, 위치를 기반으로 액세스를 제어하는 세분화된 정책을 구현할 수 있습니다.

고유한 비즈니스 요구 사항에 맞게 조정할 수 있어 계약자 액세스를 쉽게 관리하고, 위치 기반 인증을 적용하고, 액세스 관리를 간소화 할 수 있습니다. 강력한 보안 표준을 유지하면서 필요에 따라 사용자 또는 그룹에 효율적으로 액세스 권한을 부여하고 비즈니스 운영을 원활하게 할 수 있습니다.



선제적 보안을 위한 애널리틱스 활용

선제적 보안은 오늘날의 역동적인 사이버 보안 환경에서 새로운 위협에 앞서 나가기 위한 핵심 요소입니다. Ivanti Neurons for ZTA를 사용하면 조직에서 고급 분석을 활용하여 선제적 보안 조치를 취할 수 있습니다. 실시간 이상 징후 탐지 및 사용자 및 엔티티 행동 분석(UEBA)은 비정상적인 행동과 잠재적 위험을 식별하는 데 도움이 됩니다.

이 솔루션은 취약성 위험 등급(VRR) 인사이트를 활용하여 엔드포인트 취약성을 평가하므로 효과적인 위험 분류에 필요한 가시성을 제공합니다. 자동화된 조치는 정책 위반 및 위험 점수, 개선 조치에 대응하여 조직이 잠재적인 위협에 대해 잠재적인 위협에 신속하게 대응할 수 있습니다.

Ivanti Neurons for ZTA로 중요한 보안 문제를 해결하고, 제로 트러스트 액세스 모델을 자신 있게 구현하며, 애플리케이션 접근을 관리하고 제어할 수 있습니다. 또한, 강력한 분석 기능을 활용하여 선제적인 보안을 구현할 수 있습니다. 원격 액세스를 관리하거나 하이브리드 인력의 보안을 강화하거나 보안 가시성을 개선하는 등 어떤 문제를 다루든, Ivanti 솔루션이 모든 단계에서 지원해 드립니다.

기능	이점
엔드 투 엔드 액세스 정책	모든 리소스에 대한 엔드 투 엔드 액세스 정책을 정의하여 원격 사용자와 on-premise 사용자 간의 구분을 없앨 수 있습니다.
“Invisible” 게이트웨이	ZTA를 사용하면 애플리케이션 게이트웨이를 공격자가 탐지할 수 없게 만들면서, 인증 및 권한이 부여된 사용자에게 원활하게 액세스 권한을 부여할 수 있습니다.
단일창으로 가시성 확보	기업 전반의 사용자, 디바이스, 애플리케이션, 컨텍스트 및 인프라에 대한 전체적인 가시성 및 규정 준수 보고 기능을 확보할 수 있습니다.
적응형 SSO	SAML 2.0로 SaaS와 third-party 애플리케이션에 대한 SSO를 제공합니다.
지능형 트래픽 조정	자동화된 최적 게이트웨이 선택으로, 사용자의 앱 트래픽이 항상 가장 빠른 게이트웨이로 전달되도록 하여 최상의 사용자 경험을 제공합니다.
엔드 포인트 규정 준수	액세스를 허용하기 전에 사용자와 디바이스를 세분화된 정책에 따라 인증하여, 멀웨어 및 기타 위협의 위험을 최소화합니다.
애플리케이션 검색	애플리케이션 사용 현황을 종합적으로 파악하고, 엔드 유저를 방해하지 않으면서 ZTA 정책을 생성하여 애플리케이션을 효율적으로 관리합니다.
사용자 행동 분석	분석 데이터를 활용하여 보안 위험을 줄이고, 이상 징후를 감지하고, 사용자 환경을 최적화하고, 모바일 인력에 대해 대응합니다.
데이터 프라이버시 및 주권	사용자 앱 트래픽이 ZTA 제어 영역에서 분리된 고객 배포 게이트웨이를 통해 직접 흐르기 때문에 데이터 주권을 확보하여 데이터 흐름을 독점적으로 제어할 수 있습니다.
DLP 및 AV 모니터링	외부 및 관리되지 않는 리소스와의 데이터 통신을 모니터링하여 데이터 손실 및 유출을 방지하고, 엔드 장치를 손상으로부터 보호합니다.

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com

이반티 총판 에쓰티케이
No1. AI &Security Solution Company

홈페이지: stkcorp.co.kr
영업문의: ivanti.sales@stkcorp.co.kr
마케팅문의: ivanti.mkt@stkcorp.co.kr
기술문의: ivanti.tech@stkcorp.co.kr