Ivanti Neurons para Zero Trust Access

Acceso seguro para el lugar de trabajo “en cualquier parte”

Ivanti Neurons para Zero Trust Access (nZTA) crea una conexión segura desde el dispositivo a las aplicaciones web en las instalaciones y en la nube, lo que aumenta la seguridad, la productividad y el cumplimiento de la normativa, y a su vez mejora notablemente la experiencia administrativa y del usuario final.

Zero Trust Access Everywhere

Obtenga una autenticación continua de usuarios y dispositivos y acceso protegido permanente a las aplicaciones corporativas en las instalaciones, en el centro de datos y en las nubes privadas y públicas.

Autenticar y autorizar automáticamente a los usuarios, los dispositivos y la conexión de aplicaciones según a restricciones flexibles y granulares, asegurando un control adaptativo, capacidad de microsegmentación y una reducida superficie de ataque.

Mayor visibilidad y análisis

Obtenga acceso al estado en tiempo real y a las tendencias históricas y aproveche la información de uso y comportamiento de nZTA, como por ejemplo, desde dónde se conecta un usuario y qué dispositivos utiliza normalmente y a qué dispositivos accede, para así tomar medidas de forma proactiva y mitigar los riesgos de seguridad.

Optimizar la productividad y la agilidad de la empresa

Implemente nuevos servicios de forma segura y realice cambios de política granulares más rápidamente. nZTA elimina la obstrucción del tráfico y mejora la experiencia del usuario con el acceso a la aplicación. Y con un único cliente para el acceso local remoto y directo a la nube, acelere sus esfuerzos de confianza cero sin fricciones.

Elección y flexibilidad: políticas granulares y colocación de puertas de enlace

Coloque las pasarelas donde quiera. Admita hasta cinco dispositivos con cada usuario nombrado y añada un número flexible de puertas de enlace para garantizar un entorno de seguridad óptima.

Aliviar la congestión del tráfico de la red y las tarifas de peaje de datos

Con nZTA, sus datos nunca pasan por nuestra plataforma, lo que reduce la presión sobre el ancho de banda corporativo y elimina los cargos por datos en los SWGs y CASBs.

Se integra con la VPN

Aumente la productividad y evite los largos tiempos de implementación de la infraestructura o el software mediante la integración de nZTA con la VPN existente. Proporcione fácil y rápidamente acceso seguro a nuevas aplicaciones, integre nuevas unidades o facilite la actividad de fusiones y adquisiciones.

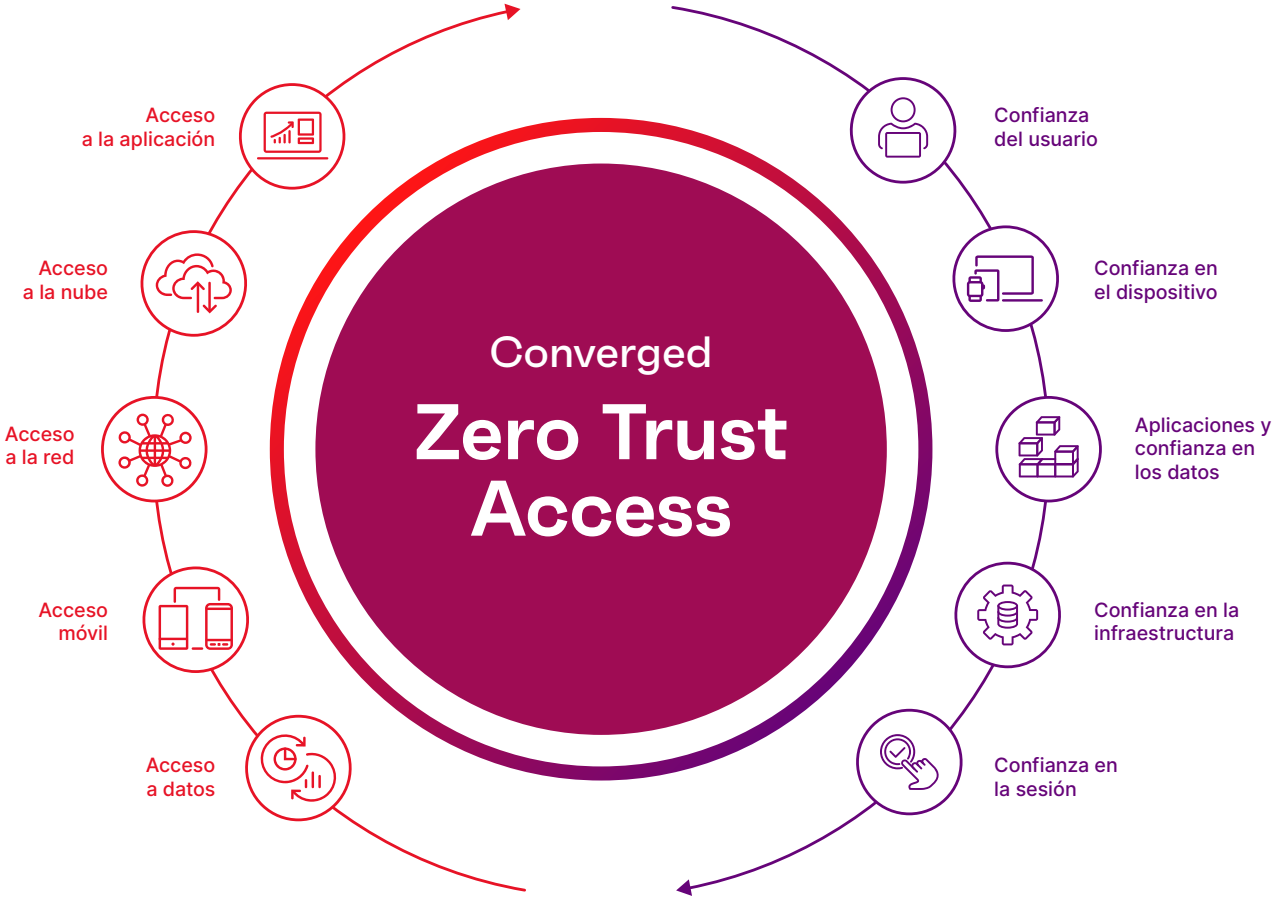
Cómo funciona

nZTA es una solución de acceso a la red de confianza cero diseñada para trabajar con su solución VPN o con organizaciones que dan prioridad a la nube.

nZTA autentifica y autoriza la identidad del usuario y la postura de seguridad del dispositivo para el cumplimiento antes de establecer una sesión. La nZTA regula cada solicitud de acceso y la sesión a través de una política desplegada y gestionada de forma centralizada y aumenta estas políticas con Análisis de Comportamiento de Usuarios y Entidades (UEBA) integrado, donde se supervisan y evalúan los atributos de cada sesión. Las puntuaciones de riesgo propias identifican las actividades no conformes, maliciosas y anómalas, lo que permite agilizar las acciones de mitigación de amenazas.

Las pasarelas nZTA se despliegan de forma flexible donde usted quiera, ya sea en las instalaciones o cerca de sus aplicaciones en la nube. Esta cercanía optimiza la experiencia del usuario, reduce la demora y permite la implementación de TI híbrida a escala. El controlador verifica las políticas de acceso en el dispositivo y gateway, creando un túnel MTLS seguro, eliminando cualquier interacción de datos con el controlador nZTA.

nZTA proporciona flexibilidad de implementación y gestión de políticas cohesivas para el desarrollo de aplicaciones en cualquier lugar, al mismo tiempo que ofrece amplias capacidades de acceso Seguro a aquellas organizaciones con entornos multinube.



Característica	Ventaja
Política de acceso de extremo a extremo	Defina políticas de acceso de extremo a extremo para cada recurso, eliminando la distinción entre usuarios remotos y locales.
Nube negra	Aplicaciones invisibles únicamente accesibles después de que el usuario y el dispositivo hayan sido autenticados y autorizados.
Visibilidad de una única pantalla	Visibilidad integral e informes de cumplimiento de usuarios, dispositivos, aplicaciones e infraestructura en toda la empresa.
Separación de los planos de control y de datos	El tráfico de usuarios y aplicaciones se envía directamente entre el usuario y la pasarela designada, lo que reduce el riesgo de pérdida de datos y mejora la experiencia del usuario.
SSO adaptativo	Integrar a través de SAML 2.0 para proporcionar SSO a las aplicaciones SaaS y 3rd de terceros compatibles.
Cumplimiento de puntos finales	El usuario y los dispositivos se autentican con políticas granulares antes de conceder el acceso, lo que reduce la posibilidad de programas malignos y otras amenazas.
Análisis del comportamiento de los usuarios	Aproveche los datos analíticos para reducir los riesgos de seguridad, detectar anomalías, optimizar la experiencia del usuario y adaptarse a las fuerzas de trabajo móviles.
Privacidad y soberanía de los datos	Todos los datos del usuario y de la aplicación están totalmente encriptados entre el cliente y la pasarela: la ZTA nunca interactúa con los datos del cliente.
Nube híbrida y local	Las puertas de enlace pueden desplegarse en la nube pública, la nube privada o los centros de datos del cliente.

ivanti

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