ivanti

Ivanti Neurons for Zero Trust Access

Accesso sicuro per l'Everywhere Workplace

Ivanti Neurons for Zero Trust Access (nZTA) dà luogo a una connessione sicura dal dispositivo alle applicazioni web-based in locale e nel cloud, e ottimizza sicurezza, produttività e compliance, migliorando al contempo l'esperienza sia degli amministratori che degli utenti finali.

Accesso Zero Trust ovunque

Assicura l'autenticazione ininterrotta di utenti e dispositivi, con accesso protetto sempre attivo ad pplicazioni aziendali in locale, nei data center e su cloud pubblici e privati.

Autentica e autorizza automaticamente la connessione di utenti, dispositivi e applicazioni in base a vincoli flessibili e granulari, con controllo adattivo, capacità di microsegmentazione e una inore superficie di attacco.

Visibilità e analitiche migliorate

Controlla lo stato in tempo reale e l'andamento storico, e sfrutta le informazioni sull'uso e sul comportamento apprese da nZTA (ad esempio, da dove accede un utente, quali ispositivi usa e a quali accede) per intervenire in modo proattivo e mitigare i rischi per la sicurezza.

Migliora la produttività e la flessibilità

Implementa nuovi servizi in tutta sicurezza e semplifica le modifiche granulari alle policy. nZTA rimuove il cosiddetto "hairpinning" del traffico e migliora l'esperienza utente grazie all'accesso diretto alle applicazioni. Inoltre, con un unico client per l'accesso locale, remoto e diretto al cloud, è possibile accelerare e agevolare la strategia zero trust.

Scelta e flessibilità: policy granulari e posizionamento di gateway

Colloca gateway ovunque tu voglia. Supporta da uno a cinque dispositivi per ogni utente designato e aggiungi un numero indefinito di gateway per garantire un mbiente sicuro ideale.

Alleggerisci il traffico di rete e riduci i costi dei dati

Con nZTA, i tuoi dati non passano mai attraverso la nostra piattaforma, riducendo il carico sulla larghezza di banda aziendale ed eliminando i costi dei dati su SWG e CASB.

Integrazione con VPN

Aumenta la produttività ed evita lunghi tempi di implementazione di infrastrutture o software, integrando nZTA alla VPN esistente. Fornisci in modo semplice e rapido l' accesso sicuro a nuove applicazioni, integra nuove unità commerciali e semplifica le attività M&A.

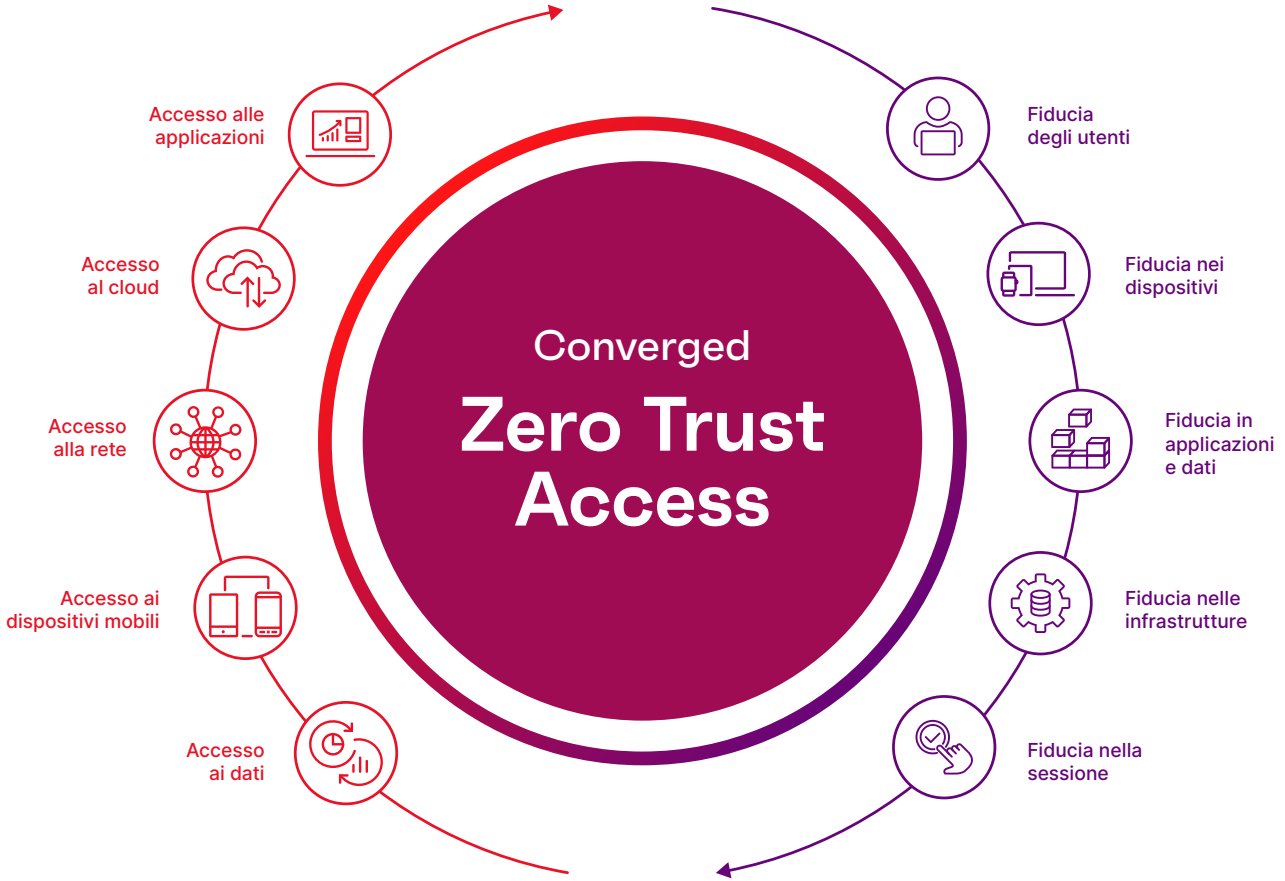
Come funziona

nZTA è una soluzione di accesso alla rete zero trust SaaS progettata per funzionare assieme alla tua soluzione VPN o con le principali soluzioni cloud.

Prima di una sessione, nZTA autentica e autorizza le identità degli utenti e lo stato di compliance dei dispositivi . nZTA gestisce ogni singola richiesta e sessione di accesso mediante policy centralizzate e potenziate con una soluzione integrata di User and Entity Behavior Analytics (UEBA). Gli attributi di ogni sessione vengono controllati ed esaminati, quindi mediante punteggi di rischio proprietari, vengono individuate le attività non conformi, dannose e anomale, consentendo di intervenire tempestivamente per mitigarele minacce.

I gateway di nZTA sono flessibili e posono essere implementati ovunque, in locale o nelle applicazioni cloud. In tal modo si ottimizza l'esperienza utente, si riducono i tempi di latenza ed è possibile adottare un'implementazione IT ibrida su larga scala. Il controller verifica le policy di accesso su dispositivo e gateway, creando un tunnel MTLS sicuro ed eliminando qualsiasi interazione dei dati con il controller nZTA.

nZTA fornisce flessibilità di implementazione e una gestione uniforme delle policy per l'implementazione di applicazioni ovunque,. Inoltre, offre capacità complete per l'accesso sicuro alle aziende che dispongono di ambienti totalmente multi-cloud.



Caratteristica	Benefici
Policy di accesso end-to-end	Definisci le policy di accesso end-to-end per ogni risorsa, eliminando la differenza tra utenti in locale e da remoto.
Dark cloud	Le applicazioni invisibili sono accessibili solo da utenti e dispositivi previamente autenticati e autorizzati.
Visibilità da un unico pannello di controllo	Visibilità complessiva e report di compliance di utenti, dispositivi, applicazioni e infrastrutture in tutta l'azienda.
Separazione del livello di controllo e dei dati	Il traffico degli utenti e delle applicazioni viene inviato direttamente dall'utente al gateway designato, riducendo il rischio di perdite di dati e migliorando l'esperienza utente.
SSO adattivo	Integrazione mediante SAML 2.0 per fornire l'SSO alle applicazioni SaaS e di terze parti.
Compliance degli endpoint	utenticazione di utenti e dispositivi rispetto a policy granulari prima di concedere l'accesso, riducendo la possibilità di malware e altre minacce.
Analisi del comportamento degli utenti	Sfrutta i dati analitici per ridurre i rischi di sicurezza, rilevare le anomalie, ottimizzare l'esperienza utente e adattarti al lavoro mobile.
Privacy e sovranità dei dati	Tutti i dati di utenti e applicazioni sono completamente criptati tra il client e il gateway: nZTA non interagisce mai con i dati del cliente.
In locale e cloud ibrido	I gateway sono implementabili su cloud pubblici o data center dei clienti.

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