Ivanti Neurons for Zero Trust Access

Secure access for the Everywhere Workplace

Ivanti Neurons for Zero Trust Access (nZTA) creates a secure connection from the device to web-based applications on-premises and in the cloud, which enhances security, productivity, and compliance while dramatically improving administrative and end user experiences.

Zero Trust Access Everywhere

Get continuous user and device authentication and always-on protected access to corporate applications on-premises, in the data center, and on private and public clouds.

Automatically authenticate and authorize users, devices, and applications connection according to flexible, granular constraints, ensuring adaptive control, micro-segmentation ability and a reduced attack surface.

Greater visibility and analytics

Gain access to real-time status and historical trends and leverage nZTA's learned usage and behavior information—e.g., where a user logs in from, what devices they normally use, and what devices they usually access—to proactively take action and mitigate security risks.

Improve business productivity and agility

Implement new services securely and make granular policy changes faster. nZTA removes traffic hair-pinning and improves user experiences with direct-to-app access. And with a single client for on-premises, remote, and direct to cloud access, accelerate your zero trust efforts without friction.

Choice and flexibility: granular policies and gateway placement

Place gateways where you want. Support up to five devices with each named user and add a flexible number of gateways to ensure your optimal security environment.

Relieve network traffic congestion and data toll charges

With nZTA, your data never goes through our platform, reducing the strain on corporate bandwidth and eliminating data charges on SWGs and CASBs.

Integrates with VPN

Boost productivity and avoid long implementation times for infrastructure or software by integrating nZTA with existing VPN. Easily and quickly provide secure access to new apps, integrate new business units, or facilitate M&A activity.

Integrates with CASB and SWG

Add core CASB and SWG features to ensure secure access to SaaS and internet applications with DLP, EDRM, OCR and malware detection.

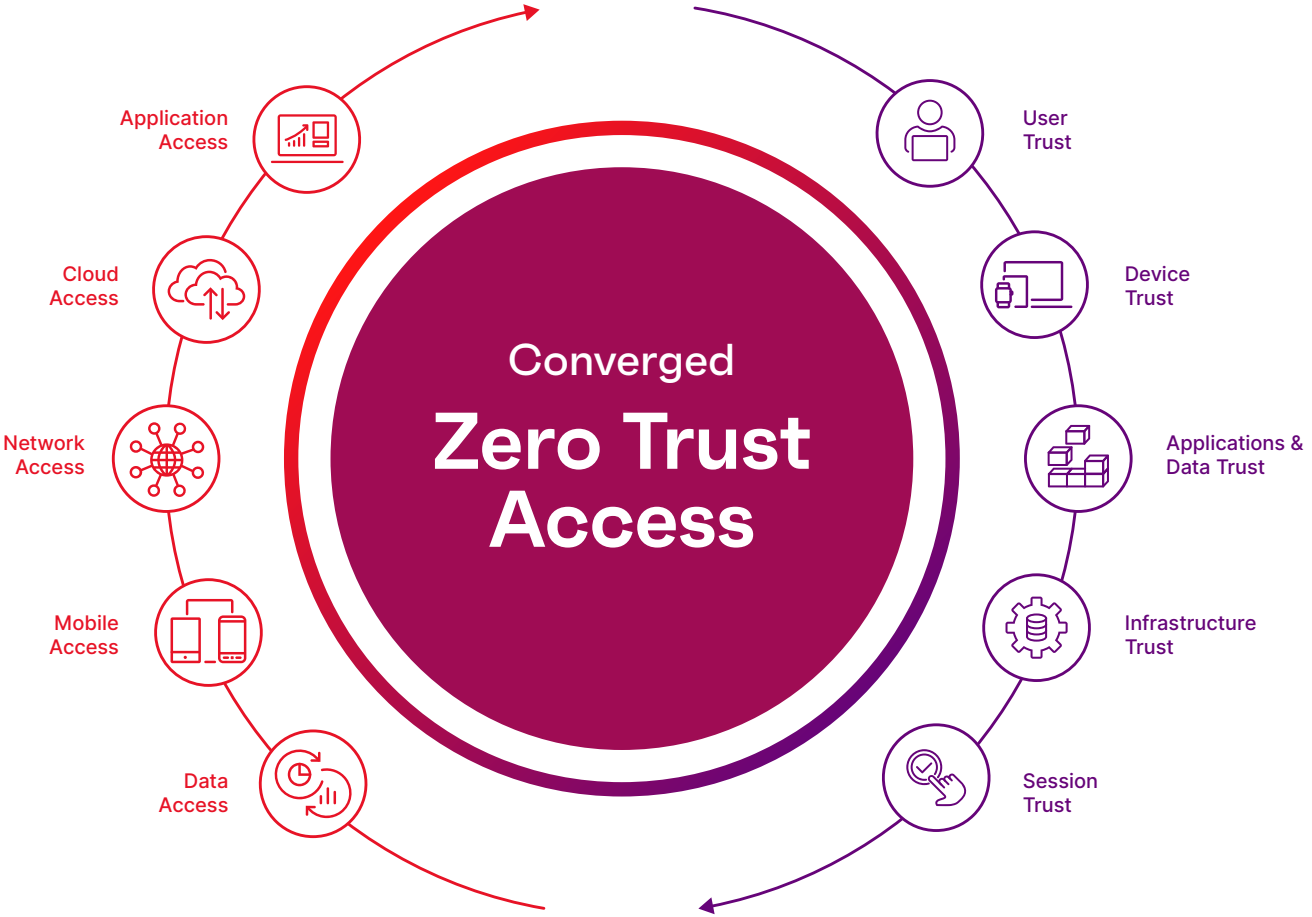
How it Works

nZTA is a SaaS-delivered zero trust network access solution designed to work with your VPN solution or with cloud-first organizations.

nZTA authenticates and authorizes user identity and device security posture for compliance before establishing a session. nZTA governs each access request and session via a centrally deployed and managed policy and augments these policies with built-in User and Entity Behavior Analytics (UEBA), where attributes for every session are monitored and assessed. Proprietary risk scores identify non-compliant, malicious, and anomalous activity—enabling expedited threat mitigation actions.

nZTA gateways are flexibly deployed where you want, either on-premises or near your cloud apps. This proximity optimizes user experience, reduces latency, and enables hybrid IT deployment at scale. The controller verifies access policies on the device and gateway, creating a secure MTLS tunnel, eliminating any data interaction with the nZTA controller.

nZTA provides deployment flexibility and cohesive policy management for application deployments anywhere while also offering comprehensive secure access capabilities to those organizations with pure multi-cloud environments.



Feature	Advantage
End-to-End Access Policy	Define end-to-end access policies for every resource, eliminating the distinction between remote and on-premises users.
Dark Cloud	Invisible applications only accessible after user and device have been authenticated and authorized.
Single Pane-of-Glass Visibility	Holistic visibility and compliance reporting of users, devices, applications and infrastructure across enterprise.
Separation of Control and Data Plane	User and application traffic are sent directly between the user and designated gateway, reducing the risk of data loss and improving user experience.
Adaptive SSO	Integrate through SAML 2.0 to provide SSO to supported SaaS and 3rd party applications.
Endpoint Compliance	User and devices authenticated against granular policies before access is granted, reducing possibility of malware and other threats.
User Behavior Analytics	Leverage analytical data to reduce security risks, detect anomalies, optimize user experience and adapt to mobile workforces.
Data Privacy and Sovereignty	All user and application data are fully encrypted between client and gateway—nZTA never interacts with customer data.
On-premises and Hybrid Cloud	Gateways can be deployed in public cloud, private cloud or customer data centers.

ivanti

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