Ivanti Neurons for Secure Access

The Secure Foundation for the Everywhere Workplace

Ivanti® Neurons for Secure Access helps customers modernize their VPN deployments by centralizing Ivanti Connect Secure (VPN) and Ivanti Neurons for Zero Trust Access management. This new cloud-based management approach provides greater control and insights into network and access status than ever before.

Deliver a Secure-Access Foundation Everywhere

Ubiquitous management of policies and environments to enable access to applications and networks

- Leverages a cloud-based management approach
- Supports a Hybrid IT model (on-prem, cloud and edge)
- Works across legacy or new Ivanti Connect Secure (VPN) and Ivanti Neurons for Zero Trust Access (ZTA) environments

Secure Access delivers ONE approach

Design and Customize Your Journey to Secure Architecture Service Edge

No vendor delivers both the ability to modernize a VPN deployment and transform into a Zero Trust architecture.

- Seamlessly integrates existing and configured VPNs
- Evolve to Zero Trust (easiest path to ZT)
- Take advantage of Ivanti's key differentiator – the Software-Defined Perimeter (SDP) architecture

Secure Access manages with ZERO configuration change required

Streamline Management

Automation and Enhanced Management = enhanced security and time savings for SecOps

- Learn from user behavior to adapt security response initially and "on the fly"
- Utilize a single pane of glass view for all gateways, users, devices, and activities
- End management overhead

Secure Access produces management-overhead time savings of 5x-20x (compared to previous VPN management)

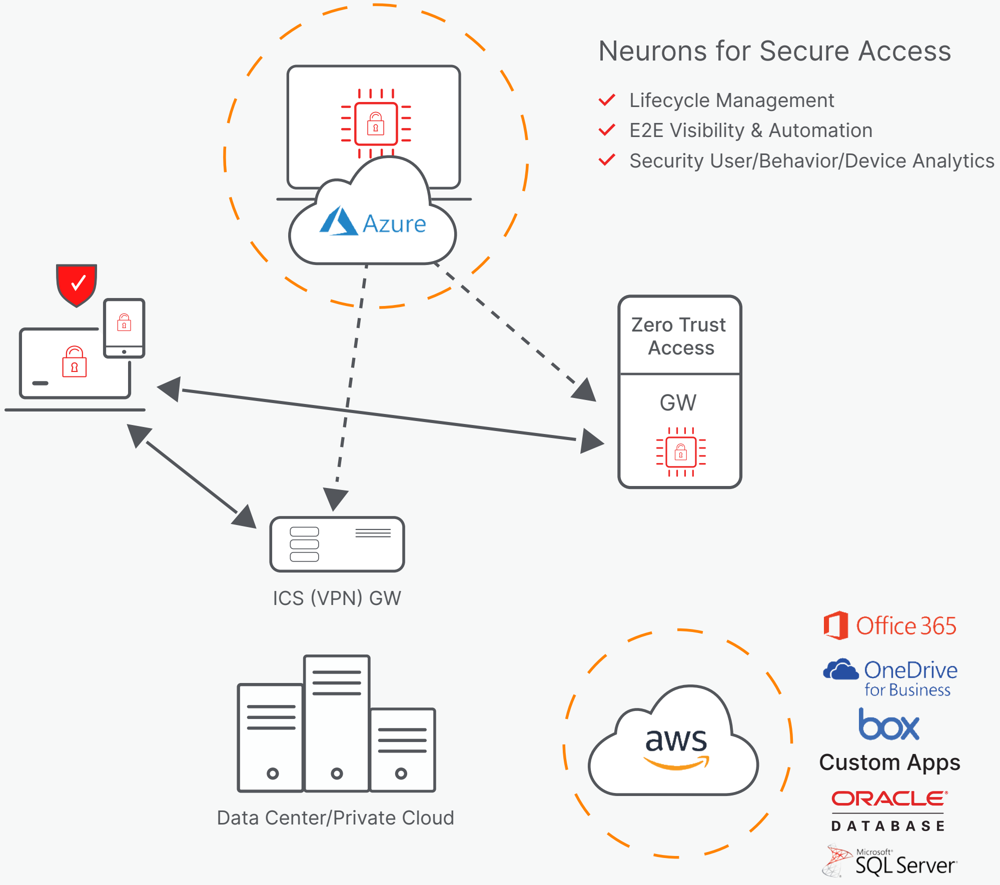
How It Works

Neurons for Secure Access (nSA) is a SaaS-delivered, centralized management and reporting platform designed to work with both Ivanti Connect Secure and Ivanti Neurons for Zero Trust Access. It provides a unified interface allowing security admins to manage multiple gateways and/or locations quickly and efficiently.

nSA simplifies workflows by consolidating all logging, reporting and activity data to a single pane of glass. Administrators gain powerful analytics tools to review the health status of their deployments as part of their daily routine. Proprietary risk scores identify non-compliant or anomalous user activity, enabling admins to identify risky user activity and react accordingly. Scheduled reports let admins design, customize and schedule reports to arrive in their inbox with the exact data they want to see.

nSA works with existing Ivanti Connect Secure (ICS) deployments and does not require additional hardware to be implemented, nor must any network or connectivity changes be made in order to integrate nSA into an ICS deployment. Registering an ICS Gateway with nSA is as simple as initiating the registration in nSA, then completing the registration on the gateway, which will initiate secure WebSocket communications between the ICS Gateway and nSA. Once connected, the ICS Gateway logs and analytics are uploaded to nSA and can be viewed and reported on from the nSA portal. Gateway-management duties allowing for the ability to upgrade, roll back and restart — as well as provide troubleshooting tools —are all enabled once ICS is connected to nSA.

Neurons for Secure Access in Action



Feature	Advantage
Secure Access Foundation	▪ Manages Connect Secure Gateways and/or Zero Trust Access Gateways in all aspects ▪ Supports both existing and next-gen VPN gateways ▪ Can co-exist with third-party VPN offerings
Gateway Lifecycle Management	▪ Enables centralized upgrades, downgrades and restarts
Configuration Management	▪ Supports gateway configurations ▪ Configuration groups for multi-node configuration management
Extensibility with Third-Party Integration	▪ Clean APIs to ease application integration (IDP, SIEM, UEM, vulnerability assessment and endpoint protection) ▪ REST APIs
Single-Pane-of-Glass Visibility	▪ Holistic visibility and compliance reporting of users, devices, applications and infrastructure across the enterprise
User Entity Behavior Analytics (UEBA)	▪ Leverages analytical data to reduce security risks, detect anomalies, optimize user experience and adapt to mobile workforces
Local (Gateway) and Central Debugging	▪ Enables getting back to business faster
Hybrid Configuration Support	▪ Gateways can be deployed in a variety of configurations including the cloud

ivanti

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