Ivanti Neurons for Secure Access

Le fondamenta sicure per l'Everywhere Workplace

Ivanti® Neurons for Secure Access aiuta i clienti a modernizzare le proprie implementazioni VPN centralizzando la gestione di Ivanti Connect Secure (VPN) e Ivanti Neurons for Zero Trust Access. Questo nuovo approccio di gestione basato sul cloud fornisce un maggiore controllo e una maggiore comprensione dello stato della rete e dell'accesso come mai in precedenza.

Garantisci delle fondamenta Secure Access ovunque

Una gestione diffusa delle politiche e degli ambienti per consentire l'accesso alle applicazioni e alle reti

- Sfrutta un approccio di gestione basato su cloud
- Supporta un modello IT ibrido (sul posto, cloud ed edge)
- Funziona in ambienti Ivanti CS (VPN) e Ivanti Neurons for ZTA legacy o nuovi

Secure Access fornisce un unico approccio

Progetta e personalizza il tuo viaggio verso SASE*

Nessun produttore offre la capacità di modernizzare un'implementazione VPN e anche di trasformarla in un'architettura Zero Trust.

- Integra facilmente una VPN esistente e configurata
- Passa a Zero Trust (il percorso più semplice verso ZT)
- Trai vantaggio dal differenziatore chiave di Ivanti - l'architettura Software-Defined Perimeter (SDP, ossia perimetro definito dal software)

Secure Access funziona senza bisogno di NESSUNA modifica alla configurazion

Gestione semplificata

Automazione e gestione migliorata = migliore sicurezza e risparmi di tempo per le SecOps

- Impara dal comportamento degli utenti ad adattare la risposta di sicurezza, sia in un primo momento che in tempo reale
- Utilizza un solo pannello di controllo per tutte le gateway, gli utenti, i dispositivi e le attività
- Elimina le spese di gestione

Secure Access comporta un risparmio in termini di tempo tra le 5 e le 20 volte nelle spese di gestione (rispetto alla gestione VPN precedente)

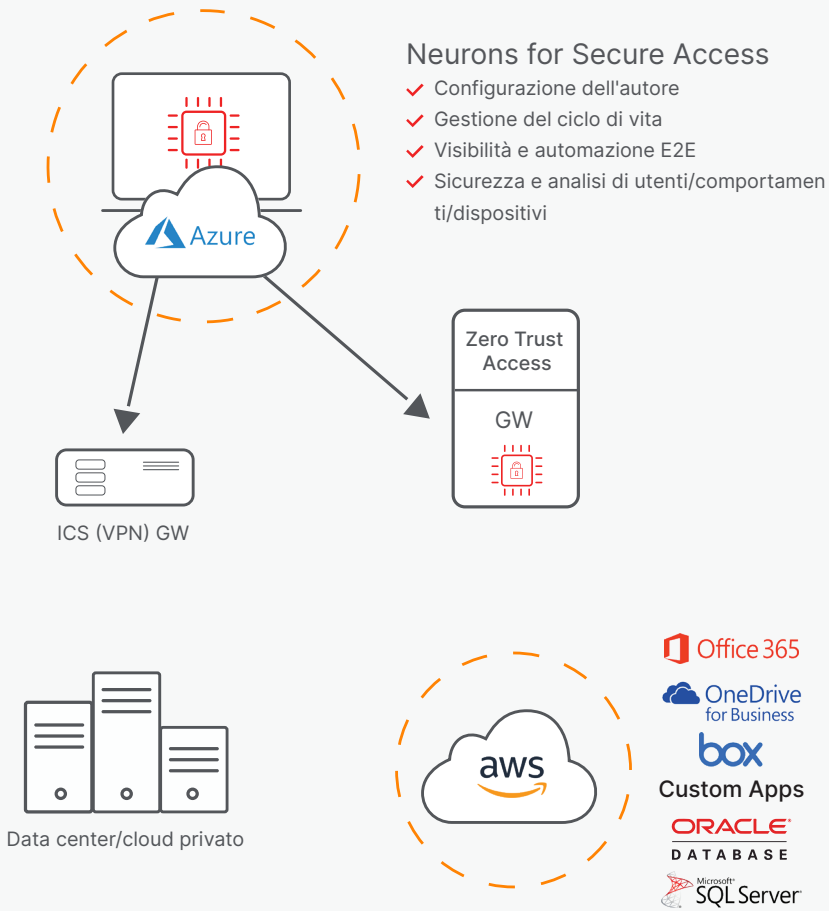
Come funziona

Neurons for Secure Access (nSA) è una piattaforma di gestione e reporting SaaS centralizzata, progettata per essere utilizzata sia con Ivanti Connect Secure che con Ivanti Neurons for Zero Trust Access. Fornisce un'interfaccia unificata che permette agli amministratori responsabili della sicurezza di gestire più gateway e/o sedi in modo rapido ed efficiente.

nSA semplifica i flussi di lavoro consolidando tutti i dati di registrazione, reporting e attività in un unico pannello di controllo, e fornisce agli amministratori potenti strumenti di analisi per rivedere lo stato delle loro implementazioni come parte della loro routine quotidiana. I punteggi di rischio proprietari identificano le attività degli utenti non conformi o anomale, dando agli amministratori la possibilità di individuare le attività degli utenti rischiose e reagire di conseguenza. Grazie ai rapporti programmati gli amministratori possono progettarli, personalizzarli e programmarli affinché inviino alla loro casella di posta elettronica esattamente i dati esatti oggi d'analisi.

nSA funziona con le implementazioni esistenti di Ivanti Connect Secure (ICS) e non richiede l'implementazione di hardware aggiuntivi o di modifiche alla rete o alla connettività, al fine di integrare l'nSA in una distribuzione ICS. La registrazione di un gateway ICS con nSA è semplice come iniziare la registrazione in nSA, per poi completare la registrazione sul gateway, che inizierà le comunicazioni websocket sicure tra il gateway ICS e nSA. Una volta connessi, i log e le analisi dell'ICS Gateway saranno caricati su nSA e potranno essere visualizzati e segnalati dal portale nSA. I compiti di gestione del gateway che permettono la capacità di aggiornamento, rollback e riavvio, oltre a fornire strumenti di risoluzione dei problemi, sono tutti abilitati una volta che l'ICS è collegato a nSA.

Neurons for Secure Access in Action



Caratteristica	Vantaggio
Fondamenta di Secure Access	■ Gestione a tutto tondo dei gateway Connect Secure e/o Zero Trust Access ■ Supporto di gateway VPN nuovi ed esistenti ■ Possibile compatibilità con proposte di VPN di terze parti
Gestione del ciclo di vita del gateway	■ Possibilità di centralizzare upgrade, downgrade e riavvii
Gestione della configurazione	■ Supporto delle configurazioni di gateway ■ Gruppi di configurazioni per la gestione di configurazioni multi-nodo
Estensibilità con integrazione di terzi	■ API puliti per semplificare l'integrazione delle applicazioni (IDP, SIEM, UEM, Vulnerability Assessment e Endpoint Protection) ■ API REST
Visibilità da un unico pannello di controllo	■ Visibilità complessiva e report di conformità di utenti, dispositivi, applicazioni e infrastrutture in tutta l'azienda
Analisi del comportamento degli utenti	■ Utilizzo di dati analitici per ridurre i rischi di sicurezza, rilevare le anomalie, ottimizzare l'esperienza utente e adattarti al lavoro mobile
Debug locale (gateway) e centrale	■ Ritorno al lavoro in tempi più rapidi
Supporto di configurazioni ibride cloud	■ I gateway possono essere distribuiti attraverso diverse configurazioni, compreso il cloud

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