

Ivanti Neurons for Secure Access

Panoramica

Ivanti Neurons for Secure Access offre gestione centralizzata e analisi dal cloud per i gateway VPN Ivanti Connect Secure (ICS). La sua interfaccia unificata controlla l'intero deployment ICS, riducendo notevolmente tempi, complessità e rischi nella gestione di deployment VPN multi-nodo. Il comportamento utente rischioso o anomalo viene affrontato con la remediation automatica, mentre i log dei gateway aggregati e i report personalizzabili forniscono informazioni operative. Neurons for Secure Access minimizza l'overhead e mantiene un ambiente sicuro per massimizzare il valore della tua VPN.

La tua implementazione VPN multi-nodo ti sta causando problemi?

Con la crescita dello smart working, molte organizzazioni hanno ampliato significativamente la propria infrastruttura VPN Ivanti Connect Secure per soddisfare la domanda degli utenti nell'Everywhere Workplace. Se da una parte questa connettività potenziata è positiva per gli utenti, l'incremento dell'overhead operativo non lo è per gli amministratori.

I grandi deployment generano complessità

Man mano che la tua organizzazione cresce, hai bisogno di una soluzione per rendere la gestione di tutto il tuo deployment di gateway VPN più semplice, non più difficile. Ti serve una modalità immediata per verificare che tutti i gateway siano in salute, aggiornati e funzionanti. Ti occorre anche una modalità per implementare rapidamente modifiche di configurazione su tutto il deployment, senza dover accedere a più interfacce, oltre che avere visibilità sulle attività di tutti gli utenti, ovunque e in qualsiasi momento si colleghino alla rete.

Segnali che hai bisogno di un migliore strumento di gestione:

- Passi ore a caricare e distribuire lo stesso aggiornamento su tutti i tuoi gateway VPN
- Una "piccola modifica di configurazione" richiede ore per essere applicata su più interfacce gateway
- La tua barra dei preferiti è tutta occupata da pagine di login dei gateway
- Ricorri a un foglio Excel ogni volta che ti chiedono un report di attività VPN multi-regione

Ivanti Neurons for Secure Access può aiutarti

Ivanti Neurons for Secure Access risolve il mal di testa del VPN multi-nodo. Non dovrai più accedere a più gateway per aggiornare una sola policy, né unire manualmente i log in un foglio Excel, né caricare lo stesso pacchetto di aggiornamento su ogni gateway. Neurons for Secure Access ti garantisce gestione configurazioni completa, gestione ciclo di vita dei gateway inclusi upgrade one-click, analisi del comportamento utente, log aggregati e troubleshooting, tutto da un unico manager cloud.

Come funziona

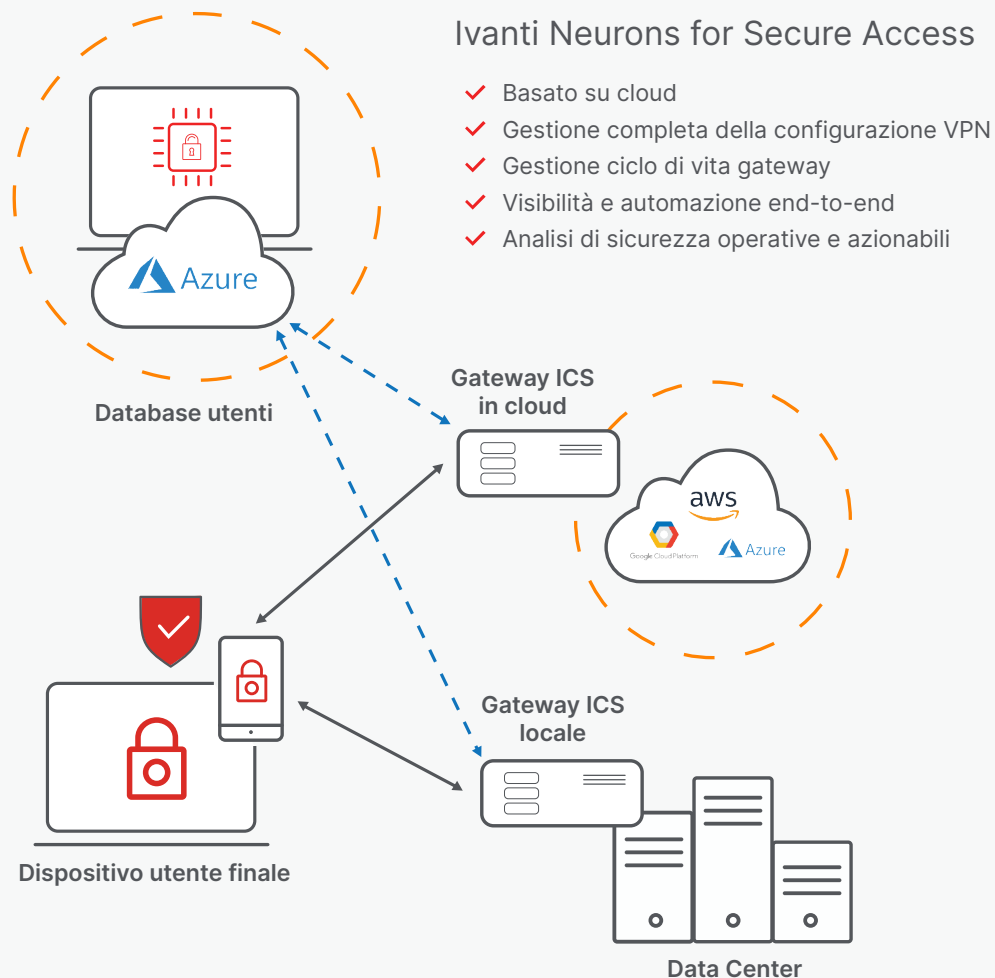
Ivanti Neurons for Secure Access è una piattaforma SaaS di gestione centralizzata e reporting per i gateway VPN Ivanti Connect Secure (ICS). Offre un'interfaccia unificata che consente agli amministratori della sicurezza di gestire rapidamente ed efficientemente tutti i deployment degli ICS gateway centralmente.

Ivanti Neurons for Secure Access semplifica i workflow e fa risparmiare tempo agli amministratori consolidando tutti i dati di configurazione, logging, reporting e attività in un'unica dashboard, eliminando la necessità di intervenire singolarmente sui gateway. Gli admin possono replicare facilmente le configurazioni tra i gateway, semplificando l'inserimento di nuovi nodi in ambiente. La gestione del ciclo di vita consente di aggiornare o effettuare il rollback di gateway, cluster o gruppi di gateway con un solo clic, riducendo drasticamente tempi e fatica necessari per distribuire gli update su tutta la VPN.

Gli amministratori hanno anche accesso agli strumenti di analisi e troubleshooting per verificare quotidianamente lo stato di salute e la sicurezza dell'intero deployment VPN. Con Application Discovery possono tracciare gli accessi applicativi sulla VPN, monitorare le metriche d'uso e analizzare i trend di accesso alle applicazioni. I report pianificati consentono agli admin di progettare, personalizzare e automatizzare report che arrivano direttamente in inbox con i dati desiderati.

Neurons for Secure Access offre una valutazione attiva dei rischi utente tramite User Entity Behavioral Analytics (UEBA), monitorando e analizzando gli attributi di ogni sessione VPN attiva per individuare comportamenti rischiosi, sospetti o anomali e assegnando un punteggio di rischio. Le informazioni ottenute permettono agli admin di configurare remediation automatica dei comportamenti a rischio, come l'applicazione di un secondo fattore di autenticazione o la quarantena del client per ulteriori verifiche.

Neurons for Secure Access è interamente ospitato su Microsoft Azure. Non è necessario installare alcun software o appliance locale. Aggiungere un gateway VPN ICS a Neurons for Secure Access è semplice come copiare un codice di registrazione e un URL nel nuovo gateway e cliccare su "join".



Funzionalità	Descrizione
External Integrity Checker Tool (ICT)	<ul style="list-style-type: none"> ■ Scannerizza da nSA verso uno o più gateway con un singolo clic ■ Utility di sicurezza progettata per verificare l'integrità dei file e dei componenti di sistema critici ■ Rileva modifiche non autorizzate, corruzione o manomissioni ■ Aiuta a identificare potenziali compromissioni o anomalie confrontando i file con baseline sicure note ■ Permette una risposta rapida alle minacce e mantiene l'affidabilità del sistema ■ Fornisce un avviso in caso di anomalia nell'ICT eseguito su un gateway ■ Permette agli admin di selezionare il pacchetto ICT per versione, eseguirlo su uno o più gateway ICS e visualizzare i risultati sulla stessa pagina
Gestione avanzata licenze funzionalità HTML5	<ul style="list-style-type: none"> ■ Permette alle organizzazioni di controllare e auditare quali tecnologie web sono disponibili per utenti o sviluppatori ■ La gestione delle licenze delle funzionalità HTML offre benefici in termini di costo, legali, di sicurezza e operativi
Secure Access Foundation	<ul style="list-style-type: none"> ■ Gestione completa dei gateway VPN Ivanti Connect Secure ■ Visibilità centralizzata e report compliance su utenti, dispositivi, applicazioni e infrastruttura dell'azienda ■ In hosting cloud su Microsoft Azure, senza alcun software o appliance locale da installare ■ Aggiorna la tua infrastruttura VPN secondo i tuoi tempi
Gateway Lifecycle Management	<ul style="list-style-type: none"> ■ Aggiornamenti, downgrade e riavvii centralizzati ■ Esperienza di upgrade "one-click" ■ Aggiornamenti di gruppo e cluster supportati ■ Suite completa di strumenti di monitoraggio e troubleshooting dei nodi gateway (es. ping, traceroute, pcap, nslookup, snapshot sistema)
Gestione Configurazione	<ul style="list-style-type: none"> ■ Gestione completamente centralizzata delle configurazioni gateway ■ "Lift and shift" di configurazioni tra gateway tramite template ■ Sincronizzazione configurazioni multi-nodo
User Entity Behavior Analytics (UEBA)	<ul style="list-style-type: none"> ■ Analisi proprietaria dei comportamenti utente per individuare attività rischiose o anomale ■ Automazione delle risposte a rischio elevato <ul style="list-style-type: none"> ■ Avviso all'utente in caso di rischio elevato ■ Forzatura dell'autenticazione secondaria ■ Negazione ulteriori login con messaggio di allerta ■ Disconnessione/disabilitazione accesso utente con messaggio di avviso

Funzionalità	Descrizione
Integrazione Server Syslog nSA	<ul style="list-style-type: none"> ■ Permette la configurazione di server syslog esterni per inoltrare i log dei gateway ICS e i log admin tenant nSA ■ Offre gestione centralizzata e sicura dei log e una visibilità maggiore su salute ed efficienza dei servizi in esecuzione nei gateway ICS
Notifiche avvisi offline	<ul style="list-style-type: none"> ■ L'amministratore tenant può configurare avvisi con indirizzi email a cui inviare notifiche
Application Discovery	<ul style="list-style-type: none"> ■ Visibilità sull'accesso applicazioni a livello L3, L4 e L7 ■ Trend negli accessi applicativi ■ Metriche di utilizzo applicazioni
Reporting personalizzato programmato	<ul style="list-style-type: none"> ■ Crea report personalizzati dai log aggregati dei gateway ed inviali via mail secondo una pianificazione
Supporto configurazione ibrida	<ul style="list-style-type: none"> ■ Crea report personalizzati dai log aggregati dei gateway ed inviali via mail secondo una pianificazione ■ Supporta gateway VPN Ivanti Connect Secure fisici, virtuali o cloud ■ Supporta gateway VPN Ivanti serie ISA ■ Coesiste con i deployment Ivanti Neurons for Zero Trust Access



Per maggiori informazioni, o per contattare Ivanti, visita [ivanti.com](https://www.ivanti.com).

Informazioni su Ivanti

Ivanti è una società di software aziendale che fornisce una piattaforma cloud completa per l'IT e la sicurezza.

Ivanti sviluppa soluzioni software scalabili in base alle esigenze dei clienti, supportando IT e Security nel migliorare l'efficienza operativa, ridurre i costi e ridurre proattivamente i rischi di sicurezza. La piattaforma Ivanti Neurons è cloud-nativa e progettata come base di servizi e strumenti unificati e riutilizzabili, per garantire visibilità, scalabilità e delivery sicuri delle soluzioni. Oltre 34.000 clienti, inclusi 85 della Fortune 100, hanno scelto Ivanti per rispondere alle sfide con soluzioni end-to-end. In Ivanti ci impegniamo a creare un ambiente in cui tutte le prospettive siano ascoltate, rispettate e valorizzate, e siamo impegnati per un futuro più sostenibile per i clienti, i partner, i dipendenti e il pianeta. Per maggiori informazioni visita [ivanti.com](https://www.ivanti.com) e segui @Golvanti.