Ivanti Neurons for Secure Access

Die sichere Grundlage für den Everywhere Workplace

Ivanti® Neurons for Secure Access unterstützt Kunden bei der Modernisierung ihrer VPN-Implementierungen durch die zentrale Verwaltung von Ivanti Connect Secure (VPN) und Ivanti Neurons for Zero Trust Access. Dieser neue Cloud-basierte Verwaltungsansatz bietet mehr Kontrolle und Einblicke in den Netzwerk- und Zugangsstatus als je zuvor.

Secure Access Foundation überall bereitstellen

Allgegenwärtige Verwaltung von Richtlinien und Umgebungen, um den Zugriff auf Anwendungen und Netzwerke zu ermöglichen

- Nutzt einen Cloud-basierten Verwaltungsansatz
- Unterstützt ein hybrides IT-Modell (On-Premise, Cloud und Edge)
- Funktioniert in alten und neuen Ivanti-CS- (VPN) und Ivanti-Neurons-for-ZTA-Umgebungen

Secure Access bietet einen Ansatz

Gestalten und individualisieren Sie Ihre Reise zu SASE*

Kein Anbieter bietet sowohl die Möglichkeit, eine VPN-Implementierung zu modernisieren als auch in eine Zero Trust-Architektur umzuwandeln.

- Einfache Integration von bestehenden und konfigurierten VPN
- Entwickeln Sie sich zu Zero Trust (der einfachste Weg zu ZT)
- Profitieren Sie von Ivantis wichtigstem Unterscheidungsmerkmal – der Software-Defined Perimeter (SDP)-Architektur

Secure Access funktioniert mit NULL Konfigurationsänderungen

Streamlining des Managements

Automatisierung und verbessertes Management = verbesserte Sicherheit und Zeitersparnis für SecOps

- Lernen Sie aus dem Benutzerverhalten, um die Sicherheitsmaßnahmen von Anfang an und „on the fly“ anzupassen.
- Nutzen Sie eine zentrale Ansicht für alle Gateways, Benutzer, Geräte und Aktivitäten
- Management-Overhead beenden

Secure Access erzeugt 5x-20x Zeitersparnis beim Verwaltungsaufwand (im Vergleich zum bisherigen VPN-Management)

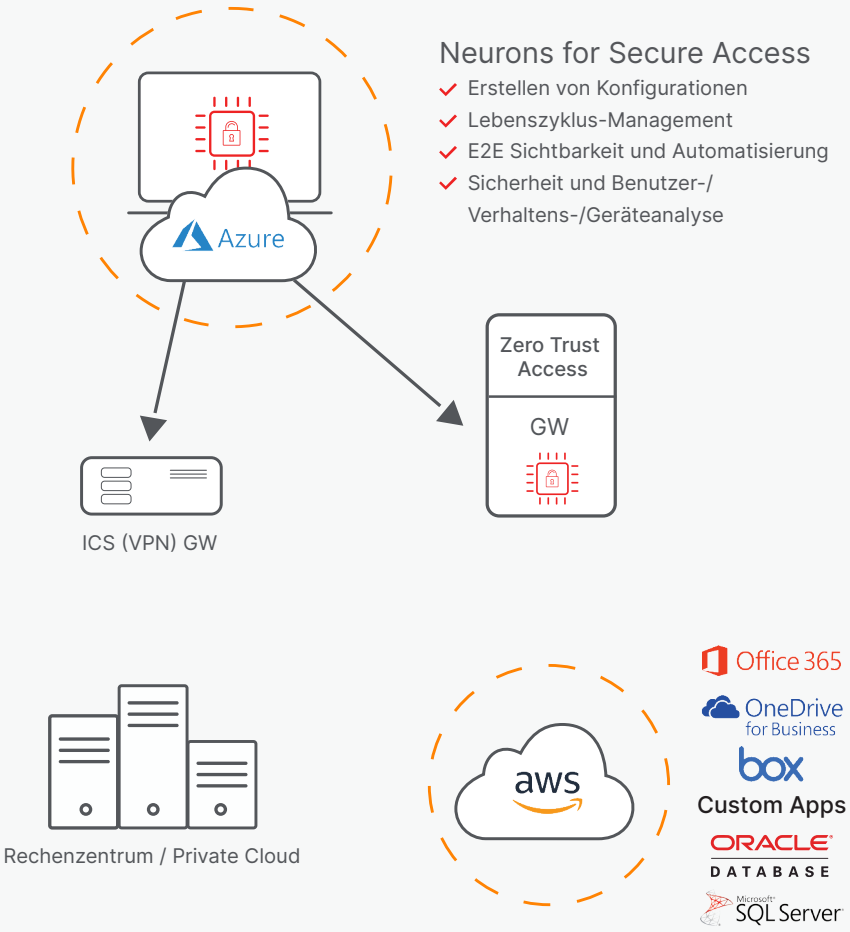
Wie es funktioniert

Neurons for Secure Access (nSA) ist eine als SaaS bereitgestellte zentralisierte Verwaltungs- und Berichterstattungsplattform, die sowohl mit Ivanti Connect Secure als auch mit Ivanti Neurons for Zero Trust Access funktioniert. Es bietet eine einheitliche Schnittstelle, über die Sicherheitsverantwortliche mehrere Gateways und/oder Standorte schnell und effizient verwalten können.

nSA vereinfacht die Arbeitsabläufe, indem es alle Protokollierungs-, Berichts- und Aktivitätsdaten in einem einzigen Fenster zusammenfasst und den Administratoren leistungsstarke Analysetools an die Hand gibt, mit denen sie den Gesundheitszustand ihrer Bereitstellungen als Teil ihrer täglichen Routine überprüfen können. Proprietäre Risikobewertungen identifizieren nicht-konforme oder anomale Benutzeraktivitäten und geben Administratoren die Möglichkeit, riskante Benutzeraktivitäten zu erkennen und entsprechend zu reagieren. Mit geplanten Berichten können Administratoren Berichte entwerfen, anpassen und so planen, dass genau die Daten in ihrem Posteingang landen, die sie sehen möchten.

nSA arbeitet mit bestehenden Ivanti Connect Secure (ICS)-Implementierungen zusammen und erfordert weder zusätzliche Hardware noch müssen Änderungen am Netzwerk oder an der Konnektivität vorgenommen werden, um nSA in eine ICS-Implementierung zu integrieren. Die Registrierung eines ICS-Gateways bei nSA ist so einfach wie das Einleiten der Registrierung in nSA und das Abschließen der Registrierung auf dem Gateway, wodurch eine sichere Websocket-Kommunikation zwischen dem ICS-Gateway und nSA initiiert wird. Sobald die Verbindung hergestellt ist, werden die ICS-Gateway-Protokolle und -Analysen zu nSA hochgeladen und können über das nSA-Portal eingesehen und ausgewertet werden. Die Gateway-Verwaltungsaufgaben, die ein Upgrade, ein Rollback und einen Neustart ermöglichen, sowie die Bereitstellung von Tools zur Fehlerbehebung sind aktiviert, sobald ICS mit nSA verbunden ist.

Neurons for Secure Access in Action



Merkmal	Vorteil
Secure Access Foundation	■ Verwaltet Connect Secure Gateways und/oder Zero Trust Access Gateways in allen Aspekten ■ Unterstützt sowohl bestehende als auch Next-Gen VPN-Gateways ■ Kann mit VPN-Angeboten von Drittanbietern zusammenarbeiten.
Gateway-Lebenszyklus-Management	■ Ermöglicht zentralisierte Upgrades, Downgrades und Neustarts
Konfigurations-Management	■ Unterstützt Gateway-Konfigurationen ■ Konfigurationsgruppen für die Verwaltung von Konfigurationen auf mehreren Knoten
Erweiterbarkeit mit Integration von Drittanbietern	■ Saubere APIs für eine einfache Anwendungsintegration (IDP, SIEM, UEM, Schwachstellenanalyse und Endpunktschutz) ■ REST-APIs
Ganzheitliche Sichtbarkeit	■ Ganzheitliche Transparenz und Konformitätsberichte über Benutzer, Geräte, Anwendungen und Infrastruktur im gesamten Unternehmen.
Verhaltensbasierte Analytik	■ Nutzen Sie analytische Daten, um Sicherheitsrisiken zu verringern, Anomalien zu erkennen, die Benutzerfreundlichkeit zu optimieren und sich an mobile Mitarbeiter anzupassen.
Lokale (Gateway) und zentrale Fehlersuche	■ Schneller zurück zum Geschäft
Unterstützung für hybride Konfigurationen	■ Gateways können in einer Vielzahl von Konfigurationen eingesetzt werden, darunter auch in der Cloud

Copyright © 2021, Ivanti. All rights reserved. IVI-2633 10/21 MA/FG/MM

ivanti

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