Ivanti Neurons for Secure Access

Überblick

Ivanti Neurons for Secure Access bietet zentrales Management und Analysen aus der Cloud für Ivanti Connect Secure (ICS) VPN-Gateways. Die einheitliche Oberfläche steuert eine gesamte ICS-Implementierung, wodurch die Zeit, Komplexität und Risiken bei der Verwaltung von Multi-Node-VPN-Implementierungen erheblich reduziert werden. Riskantes oder anomales Benutzerverhalten wird durch automatisierte Behebung adressiert, während zusammengeführte Gateway-Logs und anpassbare Berichte umsetzbare Erkenntnisse liefern. Neurons for Secure Access minimiert den Verwaltungsaufwand und gewährleistet eine sichere Umgebung, um den Nutzen Ihres VPNs zu maximieren.

Bereitet Ihnen Ihre Multi-Node-VPN-Implementierung Kopfschmerzen?

Mit der Zunahme des Homeoffice-Trends haben viele Organisationen ihre Ivanti Connect Secure VPN-Infrastruktur ausgeweitet, um dem gestiegenen Bedarf der Nutzer im Everywhere Workplace gerecht zu werden. Während die verbesserte Konnektivität für Nutzer positiv ist, stellt der erhöhte operative Aufwand für Administratoren eine Herausforderung dar.

Große Bereitstellungen können Komplexität verursachen

Wenn Ihr Unternehmen weiter wächst, benötigen Sie eine Möglichkeit, Ihr gesamtes VPN-Gateway-Deployment einfacher – nicht komplizierter – zu verwalten. Sie brauchen einen klaren Überblick, um sicherzustellen, dass alle Gateways gesund, aktuell und voll funktionsfähig sind. Ebenso benötigen Sie die Möglichkeit, Konfigurationsänderungen unkompliziert im gesamten Deployment durchzuführen, ohne sich mehrfach in verschiedene Benutzeroberflächen einzuloggen, und Sie brauchen vollständige Transparenz über die Aktivitäten aller Nutzer, unabhängig davon, wann und wo diese sich mit Ihrem Netzwerk verbinden.

Anzeichen dafür, dass Sie ein besseres Verwaltungstool benötigen:

- Sie verbringen Stunden damit, dasselbe Update auf all Ihre VPN-Gateways hochzuladen und auszurollen
- Eine „kleine Konfigurationsänderung“ benötigt Stunden, um sie auf mehreren Gateway-Oberflächen umzusetzen
- Ihre gesamte Lesezeichenleiste ist mit Gateway-Anmeldeseiten belegt
- Sie greifen jedes Mal auf Ihre Tabellenkalkulation zurück, wenn Sie nach einem VPN-Aktivitätsbericht aus mehreren Regionen gefragt werden

Ivanti Neurons for Secure Access kann helfen

Ivanti Neurons for Secure Access löst das Multi-Node-VPN-Problem. Sie müssen sich nicht mehr in mehrere Gateways einloggen, um eine einzelne Richtlinie zu aktualisieren, Datenprotokolle manuell zusammenfügen oder dasselbe Upgrade-Paket auf jedes einzelne Gateway hochladen. Neurons for Secure Access bietet Ihnen vollständige Konfiguration, Lifecycle-Management der Gateways inklusive Ein-Klick-Upgrades, Analyse des Benutzerverhaltens, zusammengeführte Protokolle und Fehlerbehebung – alles über einen einzigen, cloudbasierten Manager.

Funktionsweise

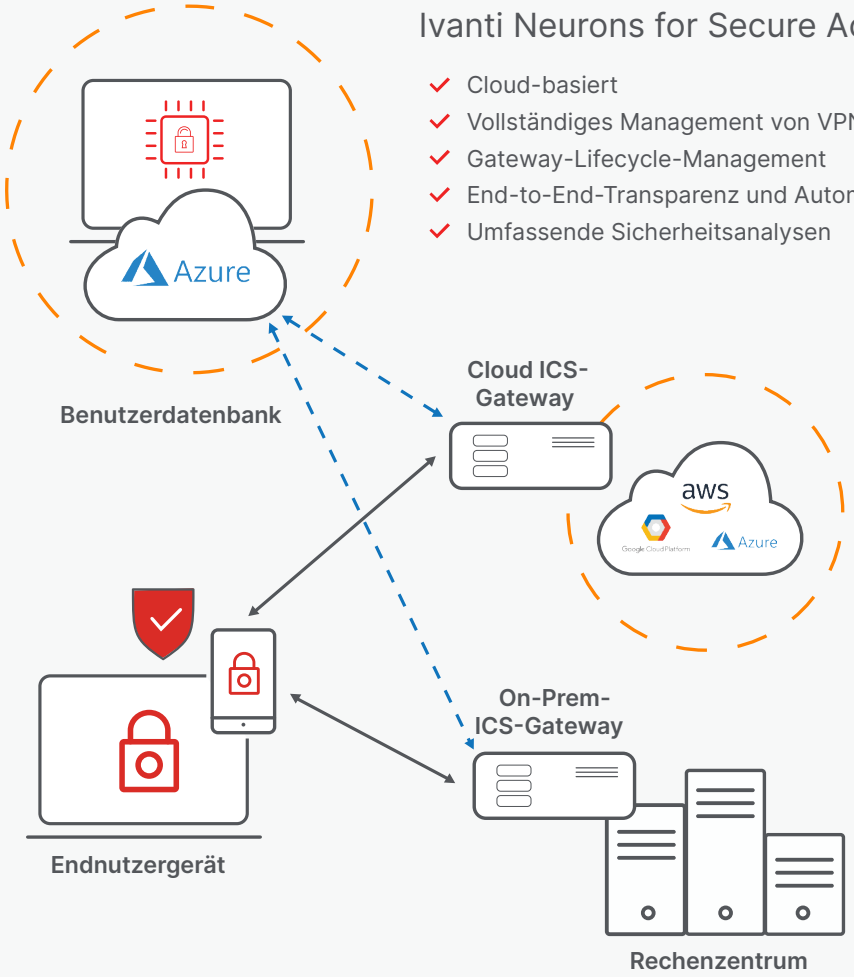
Ivanti Neurons for Secure Access ist eine SaaS-basierte, zentrale Management- und Reporting-Plattform für Ivanti Connect Secure (ICS) VPN-Gateways. Sie bietet eine einheitliche Oberfläche, die es Security-Administratoren ermöglicht, ihre gesamten ICS-Gateway-Bereitstellungen zentral, schnell und effizient zu verwalten.

Ivanti Neurons for Secure Access vereinfacht Arbeitsabläufe und spart Administratoren Zeit, indem alle Gateway-Konfigurationen, Protokolle, Berichte und Aktivitätsdaten in einer einzigen Ansicht zusammengeführt werden und die Notwendigkeit entfällt, Änderungen an einzelnen Gateways vorzunehmen. Administratoren können Konfigurationen über Gateways hinweg einfach replizieren, wodurch die Konfiguration neuer Gateways in ihrer Umgebung erleichtert wird. Das Lifecycle-Management der Gateways umfasst die Möglichkeit, Gateways, Cluster oder Gruppen von Gateways per Ein-Klick-Upgrade oder Rollback zu aktualisieren, was den Aufwand und die Zeit für das Ausrollen von Updates in der VPN-Umgebung erheblich reduziert.

Administratoren haben zudem Zugriff auf Analyse- und Fehlerbehebungstools, um den Sicherheits- und Gesundheitsstatus der gesamten VPN-Implementierung als Teil ihrer täglichen Routine zu überprüfen. Mit Application Discovery können Administratoren den Zugriff auf Anwendungen über das VPN nachverfolgen, Nutzungsmetriken überwachen und Trends beim Applikationszugriff erkennen. Geplante Berichte ermöglichen es Admins, Reports zu entwerfen, anzupassen und zu automatisieren, sodass sie mit den gewünschten Daten im Posteingang landen.

Neurons for Secure Access bietet eine verwertbare Bewertung des Benutzerrisikos mittels User Entity Behavioral Analytics (UEBA), wobei die Attribute jeder aktiven VPN-Sitzung überwacht und auf riskantes, verdächtiges oder anomales Benutzerverhalten analysiert werden und ein Risikowert zugeordnet wird. Die gewonnenen Einblicke ermöglichen es Administratoren, automatisierte Maßnahmen zur Behebung riskanten Nutzerverhaltens zu konfigurieren, wie z. B. die Durchsetzung einer Zweit-Authentifizierung oder die Quarantäne des Clients zur weiteren Überprüfung.

Neurons for Secure Access wird vollständig in Microsoft Azure gehostet. Es muss keine lokale Software oder Hardware installiert werden. Das Hinzufügen eines ICS VPN-Gateways zu Neurons for Secure Access ist so einfach wie das Kopieren eines Registrierungscodes und einer URL in das neue Gateway und das Klicken auf „Beitreten“.



Ivanti Neurons for Secure Access

- Cloud-basiert
- Vollständiges Management von VPN-Konfigurationen
- Gateway-Lifecycle-Management
- End-to-End-Transparenz und Automatisierung
- Umfassende Sicherheitsanalysen

Funktion	Beschreibung
External Integrity Checker Tool (ICT)	■ Scans von nSA auf einzelne oder mehrere Gateways mit nur einem Klick ■ Sicherheitswerkzeug zur Überprüfung der Integrität zentraler Dateien und Systemkomponenten ■ Erkennt unautorisierte Änderungen, Korruption oder Manipulationen ■ Hilft bei der Identifizierung möglicher Kompromittierungen oder Anomalien durch Vergleich von Dateien mit bekannten Referenzwerten ■ Ermöglicht schnellere Reaktion auf Bedrohungen und erhöht die Zuverlässigkeit des Systems ■ Gibt einen Alarm aus, wenn bei der durchgeführten ICT auf einem Gateway eine Anomalie festgestellt wurde ■ Ermöglicht es Admins, ein versionsspezifisches ICT-Paket auszuwählen, gegen eines oder mehrere ICS-Gateways auszuführen und die Ergebnisse auf derselben Seite einzusehen, auf der ICT ausgeführt wird
Erweiterte HTML5 Feature License-Verwaltung	■ Organisationen können steuern und überprüfen, welche Webtechnologien Nutzer und Entwickler nutzen können ■ Die Verwaltung von HTML-Feature-Lizenzen bringt Kosten-, rechtliche, Sicherheits- und betriebliche Vorteile
Secure Access Foundation	■ Vollständige Verwaltung der Ivanti Connect Secure VPN-Gateways ■ Zentrale Sichtbarkeit und Compliance-Berichterstattung zu Nutzer, Geräte, Anwendungen und Infrastruktur im gesamten Unternehmen ■ Cloud-gehostet in Microsoft Azure – keine lokale Software oder Hardware notwendig ■ Aktualisieren Sie Ihre VPN-Infrastruktur in Ihrem eigenen Tempo
Gateway-Lifecycle-Management	■ Zentralisierte Upgrades, Downgrades und Neustarts möglich ■ One-Click-Upgrade-Erfahrung ■ Gruppen- und Cluster-Upgrades werden unterstützt ■ Umfassende Monitoring- und Fehlerbehebungstools (z. B. Ping, Traceroute, pcap, nslookup, System-Snapshots)
Konfigurationsmanagement	■ Vollständig zentrales Management von Gateway-Konfigurationen ■ „Lift and Shift"-Konfigurationen zwischen Gateways per Konfigurationsvorlagen ■ Konfigurationssynchronisierung für Multi-Node-Management

Benutzerverhaltensanalytik (UEBA)	■ Eigenentwickelte Analyse des Benutzerverhaltens zur Identifizierung riskanter oder anomaler Nutzeraktivitäten
	■ Automatisierte Reaktionen auf erhöhtes Risiko
	  ■ Warnung des Nutzers bei erhöhtem Risiko
	  ■ Erzwingen der sekundären Authentifizierung
	  ■ Verweigerung weiterer Logins mit Warnmeldung
	  ■ Trennen / Deaktivieren des Nutzerzugangs mit Warnmeldung

Funktion	Beschreibung
nSA Syslog-Server-Integration	■ Ermöglicht die Konfiguration eines externen Syslog-Servers, um ICS-Gateway-Logs und nSA-Tenant-Admin-Protokolle weiterzuleiten ■ Bietet zentrales und sicheres Log-Management sowie verbesserte Transparenz zur Gesundheit und Effizienz der auf ICS-Gateways laufenden Dienste
Offline-Benachrichtigungen	■ Tenant-Admins können Alarme mit E-Mail-IDs konfigurieren, um die Empfänger zu definieren
Application Discovery	■ L3-, L4- und L7-Anwendungstransparenz ■ Trends beim Applikationszugriff ■ Anwendungsnutzungsmetriken
Individuelle, zeitgesteuerte Berichte	■ Erstellung individueller Berichte aus zusammengeführten Gateway-Protokollen zur E-Mail-Zustellung nach definiertem Zeitplan
Hybrid-Konfigurationsunterstützung	■ Erstellung individueller Berichte aus zusammengeführten Gateway-Protokollen zur E-Mail-Zustellung nach definiertem Zeitplan ■ Unterstützt physische, virtuelle oder Cloud-basierte Ivanti Connect Secure VPN-Gateways ■ Unterstützt Ivanti ISA-Series VPN-Gateways ■ Koexistenz mit Ivanti Neurons for Zero Trust Access möglich

Über Ivanti

Ivanti ist ein Unternehmenssoftwareanbieter, der eine umfassende Cloud-basierte IT- und Sicherheitsplattform bereitstellt. Ivanti bietet Softwarelösungen, die mit den Anforderungen unserer Kunden skalieren und es IT und Security ermöglichen, die betriebliche Effizienz zu steigern, Kosten zu senken und Sicherheitsrisiken proaktiv zu minimieren. Die Ivanti Neurons Plattform ist Cloud-nativ und als Grundlage für einheitliche und wiederverwendbare Services und Tools konzipiert, für konsistente Transparenz, Skalierbarkeit und sichere Bereitstellung von Lösungen. Über 34.000 Kunden, darunter 85 der Fortune 100, haben sich für Ivanti entschieden, um Herausforderungen mit End-to-End-Lösungen zu meistern. Bei Ivanti schaffen wir ein Umfeld, in dem alle Perspektiven gehört, respektiert und geschätzt werden, und wir engagieren uns für eine nachhaltigere Zukunft für unsere Kunden, Partner, Mitarbeitenden und den Planeten. Weitere Informationen erhalten Sie unter ivanti.com und folgen Sie @GoIvanti.

ivanti

Weitere Informationen oder Kontakt zu Ivanti finden Sie unter ivanti.com.