Ivanti Neurons for Secure Access

Everywhere Workplace (場所にとらわれない働き方) を実現するセキュアな基盤

Ivanti® Neurons for Secure Access は、Ivanti Connect Secure (VPN)とIvanti Neurons for Zero Trust Access (nZTA) の管理を一元化し、お客様のVPN導入の近代化を支援します。 この新しいクラウドベースの管理アプローチにより、これまで以上に優れたネットワークとアクセスの制御とインサイトを提供します。

あらゆる場所からのセキュアなアクセスを実現

アプリケーションやネットワークへのアクセスを可能にするポリシーと環境のユビキタスな管理

- クラウドベースの管理アプローチを活用
- ハイブリッド IT モデルをサポート
- 従来製品または新しいIvanti Connect Secure (VPN)とIvanti Neurons for Zero Trust Access (nZTA) 環境で動作

One アプローチを実現する SecureAccess

セキュアアーキテクトサービスエッジへの移行のデザインとカスタマイズ

VPN 導入の近代化とゼロトラストアーキテクトへの移行の両方の機能を提供するベンダーは他にいません。

- 既存の設定済みの VPN のシームレスな統合
- ゼロトラストへの進化
- Ivanti の重要な差別化要因である Software-Defined Perimeter (SDP) アーキテクチャを活用

構成の変更を必要とせずに管理する SecureAccess

効率的なマネジメント

自動化と強化されたマネジメント =SecOps による、より強固なセキュリティと運用効率を実現

- ユーザーの振る舞いを検知し、初期および稼働中にセキュリティ対応を適応
- すべてのゲートウェイ、ユーザー、デバイス、アクティビティを単一の画面で表示
- 管理オーバーヘッドを削減

Secure Access により、管理オーバーヘッド時間を従来のVPN管理と比較して5倍から20倍削減

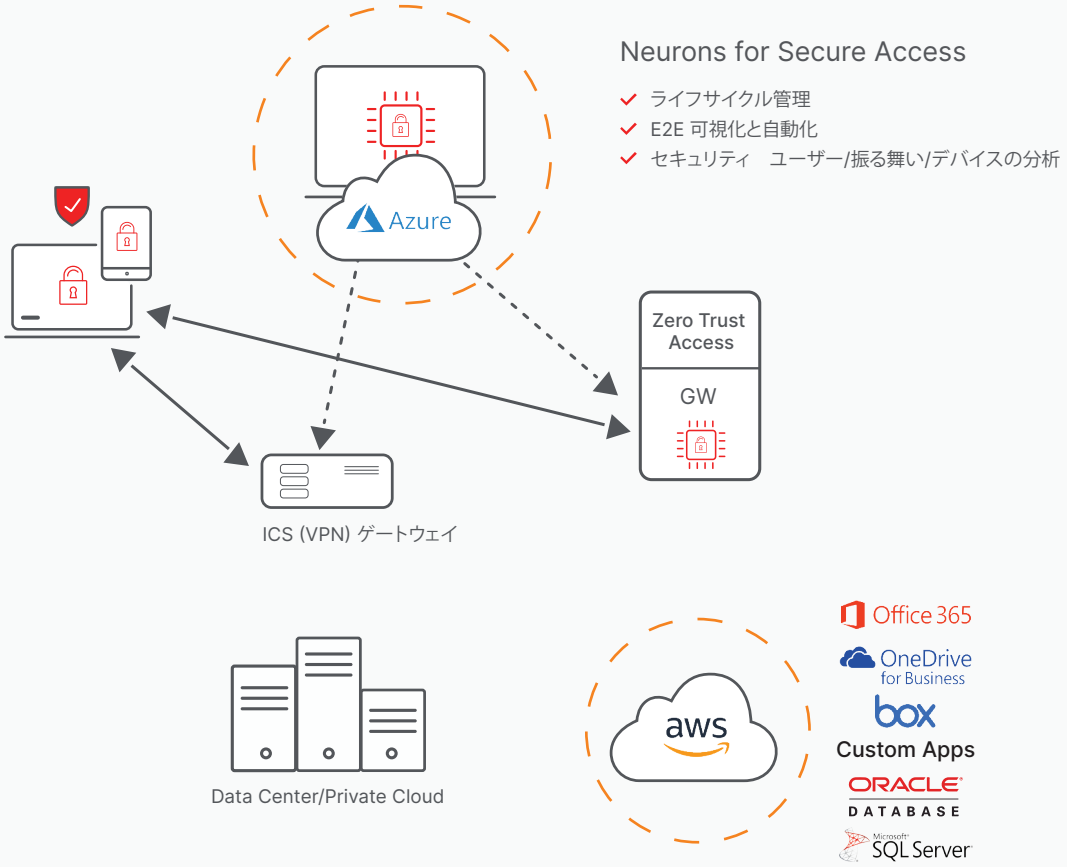
仕組み

Neurons for Secure Access（nSA）は、Ivanti Connect SecureとIvanti Neurons for Zero Trust Accessの両方で動作するように設計された、SaaS型の一元管理・レポートティングプラットフォームです。 統一されたインターフェイスにより、セキュリティ管理者は複数のゲートウェイやロケーションを迅速かつ効率的に管理することができます。

nSAは、すべてのログ、レポート、およびアクティビティデータを単一の画面に統合することで、ワークフローを簡素化します。管理者は、強力な分析ツールによって、常時システムの健全性を確認することができます。管理者は、独自のリスクスコアにより、コンプライアンス違反や異常なユーザーアクティビティを特定し、リスクの高いユーザーアクティビティを識別して、それに応じた対応することができます。スケジュールレポートは、管理者が構成・カスタマイズし必要なデータを抽出したレポートを通知することができます。

nSAは既存のIvanti Connect Secure (ICS) と連携して動作するため、追加のハードウェアを実装する必要はありません。また、nSAをICSに統合するためにネットワークや接続を変更する必要もありません。ICSゲートウェイのnSAへの登録は、nSAで登録を開始し、ゲートウェイで登録を完了させるだけで、簡単に行えます。それだけで、ICS ゲートウェイとnSA の間でセキュアなWebSocket 通信を開始されます。接続後、ICS ゲートウェイのログと分析結果がnSAにアップロードされ、nSAポータルから閲覧やレポートティングが可能となります。ICSをnSAに接続すると、アップグレード、ロールバック、再起動、およびトラブルシューティングツールなどのゲートウェイ管理機能がすべて有効になります。

Neurons for Secure Access の仕組み



機能	メリット
セキュアアクセスの基盤	■ Connect Secure GW および/または Zero Trust GW を管理 ■ 既存と次世代の VPN ゲートウェイ両方をサポート ■ サードパーティー VPN 製品と共存
ゲートウェイライフサイクル管理	■ アップグレード、ダウングレード、再起動の集中管理
構成管理	■ ゲートウェイの設定をサポート ■ マルチノード構成管理のための構成グループ
サードパーティーとの統合による拡張性	■ アプリケーションの統合を容易にするクリーンな API（IDP、SIEM、UEM、脆弱性評価、エンドポイント保護） ■ REST API
単一画面での可視化	■ 企業内のユーザ、デバイス、アプリケーション、インフラストラクチャの全体的な可視化とコンプライアンスに関するレポートティング
ユーザーおよびエンティティの振る舞い分析 (UEBA)	■ 分析データを活用し、セキュリティリスクの低減、異常の検出、ユーザ体験の最適化、モバイル従業員への適応
ローカル (ゲートウェイ)および セントラルデバッギング	■ 迅速な業務復旧
ハイブリッド構成のサポート	■ ゲートウェイは、クラウドを含むさまざまな構成に対応

ivanti.co.jp
+81 (0)3-6432-4180
contact@ivanti.co.jp