Everywhere Workplaceのための ゼロトラスト ネットワークアクセス

Ivanti Neurons for Zero Trust Access (nZTA)は、Lookoutと提携し、オンプレミス、プライベートおよびパブリッククラウド、オープンインターネットなど、高度に分散したアプリケーションエコシステムにおいて、ゼロトラストによる安全なアクセスと可視化を提供するとともに、ユーザーとそのデータ、デバイスを偶発的または悪意のあるデータ流出やウイルス、マルウェア、ランサムウェアなどの脅威から保護することができます。

ユーザーとそのデータをプロアクティブに保護するにはどうすればよいのでしょうか？

Everywhere Workplace（場所にとらわれない働き方）において、企業はユーザーとの繋がりや利便性を求め、益々クラウドアプリケーションに頼るようになっています。こうしたクラウドアプリケーションは、あらゆるデバイスからのアクセスを可能にし、ユーザーがどこから働いても生産性を上げられるようにします。このような便利さの中、すべての企業が直面せざるをえない新たな課題も生まれています。

- オンプレミスとクラウドにあるアプリケーションへのアクセスをどのように管理・制御しますか？
- ユーザーはどのように会社の機密データを扱っているのか、そのデータはどこに流れいるのか、そしてどのようにそれを特定できるのでしょうか？
- ユーザーデバイスや個人用アプリが、企業をリスクにさらしていないか？

Everywhere Workplaceでの可視化とコントロール

企業は、クラウドアプリケーションに依存するようになるにつれて、機密データが悪意のあるユーザーの手に渡らないように保護しながら、ユーザー、デバイス、およびユーザーが使用するアプリケーションの安全性、セキュリティ、や生産性を確保する必要があります。企業は、社内アプリケーションへのアクセスを必要なユーザーのみに制限し、エンドユーザーにシームレスなエクスペリエンスを提供する必要があります。また、企業は、機密性の高いデジタル資産を保護し、データの所在や使用者にかかわらず規制に準拠し続ける必要があります。そのためには、ユーザー、ユーザーのデバイス、データの安全性を確保、可視化を実現し、安心できるようにする必要があります。

セキュアアクセスと機密データの保護

nZTAは、どこからでも、どのデバイスからでも、オンプレミス、プライベートおよびパブリッククラウド上の企業アプリケーションへの安全なオンデマンドのアクセスを可能にします。柔軟できめ細かいポリシーに基づき、ユーザー、デバイス、アプリケーション接続の認証と承認を自動的に行い、ユーザーが必要な時に必要なアプリケーションにアクセスできるようにします。アプリケーション毎のマイクロセグメンテーション制御で横方向の脅威を防ぎ、UEBA（User and Entity Behavioral Analytics/ユーザーおよびエンティティの行動分析）でリスクのあるユーザー行動を問題になる前に特定することができます。

IvantiとLookoutの提携により、インターネットやSaaSアプリケーション向けにデータ損失防止（DLP）、エンタープライズデジタル著作権管理（E-DRM）、光学文字認識（OCR）、完全データ一致（EDM）、マルウェア検出、インシデント対応、データ分類を追加し、機密データやデジタル資産を事故や悪意による漏えいから保護します。

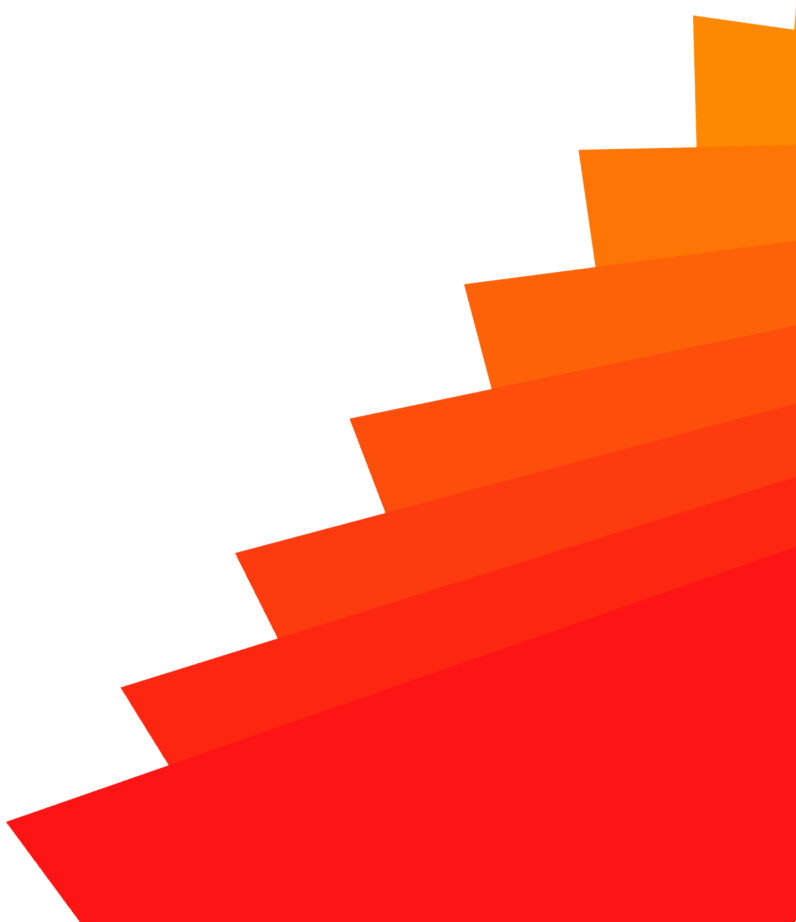
仕組み

Neurons for Zero Trust Access（nZTA）は、VPNソリューションやクラウドファーストの環境と連携できるように設計された、SaaS型のゼロトラストネットワークアクセスソリューションです。

nZTAは、アプリケーションのセッションを確立する前に、クラウド上にあるnZTAコントローラで、ユーザーIDとデバイスのセキュリティポスチャを認証・承認します。nZTAは、一元的に展開および管理されるポリシーエンジンによって各アクセスリクエストとセッションを管理し、搭載されたユーザーおよびエンティティの行動分析（UEBA）でポリシーを強化し、各セッションの属性を監視・評価します。独自のリスクスコアにより、コンプライアンス違反や、悪意のある行動または異常な行動を特定し、脅威に対する迅速な対応が可能になります。

nZTAゲートウェイは、オンプレミス、パブリックまたはプライベートクラウド環境に柔軟に導入でき、ユーザーエクスペリエンスを最適化し、レイテンシーを低減させ、大規模なハイブリッドITの展開を可能にします。nZTAコントローラはアプリケーションのアクセスポリシーを確認してから、デバイスとnZTAゲートウェイの間に直接セキュアにアプリケーション毎のmTLSトンネルを作成するようIvanti Unified Clientに指示し、nZTAコントローラとのデータのやり取りを排除します。Ivanti Unified Clientは、アプリケーショントンネルを接続するために最適なゲートウェイにトラフィックを自動的に誘導します。コストのかかるトラフィックのバックホールやヘアピニングは必要ありません。

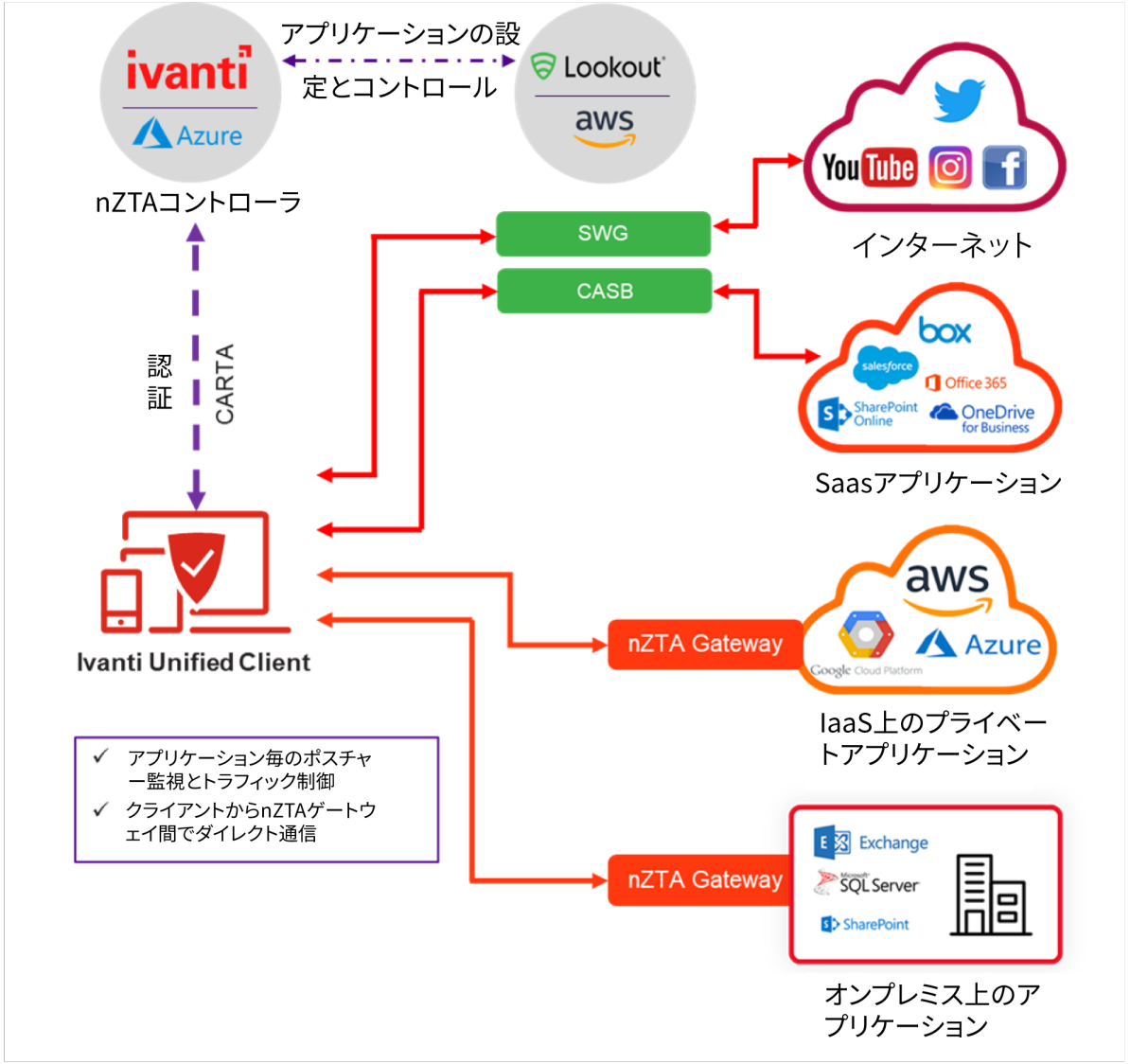
nZTAは、Lookoutとの提携により、インターネットやSaaSベースのクラウドサービス、ユーザー、デバイスを介して機密データとドキュメントをリアルタイムで特定、分類、保護することが可能になります。一元化されたデータ損失防止（DLP）ポリシーを通じて、個人識別情報（PII）、保護対象保健情報（PHI）、クレジットカード業界（PCI-DSS）データとして分類された情報などの規制データとの整合性を維持しながら、あらゆるクラウド環境、電子メール、アプリケーションにわたって機密データを一貫して検出、分類、保護することができます。



ivanti

エンタープライズデジタル著作権管理（E-DRM）により、ダウンロード、保存、共有されるファイルを自動的に暗号化し、適切なアクセス権を持つユーザーのみが安全にアクセスできるようにすることで、機密ファイルを保護できます。インバウンドおよびアウトバウンドのマルウェア検出と自動検疫により、ユーザーを保護し、ウイルス、マルウェア、ランサムウェアの攻撃を阻止します。また、行動分析により異常な行動を特定し、潜在的な脅威を修正することができます。

Neurons for Zero Trust Accessは、あらゆる場所にアプリケーションを展開するための柔軟性と一貫したポリシー管理を実現すると同時に、マルチクラウド環境を持つ組織に包括的なセキュアアクセス機能を提供します。Lookoutは、ユーザーのクラウドやインターネットアプリケーションに従来難しかった可視化を実現し、機密データの漏洩を防ぐとともに、悪意のある脅威からユーザーとそのデバイスを保護します。



機能	概要
エンドツーエンドのアクセスポリシー	リモートユーザーとオンプレミスユーザーの区別をなくし、すべてのリソースに対してエンドツーエンドのアクセスポリシーを定義することができます。
コントロールプレーンとデータプレーンの分離	ユーザーおよびアプリケーションのトラフィックは直接ユーザーと指定されたゲートウェイの間で送信され、データ損失のリスクを低減しユーザーエクスペリエンスを向上させます。
オンプレミスとハイブリッドクラウド	ゲートウェイはパブリッククラウド、プライベートクラウド、データセンターのいずれにも導入できます。
アダプティブシングルサインオン	SAML 2.0に統合し、サポートされるSaaSおよびサードパーティアプリケーションにSSOを提供します。
エンドポイント・コンプライアンス	ユーザーとデバイスをきめ細かいポリシーに基づいて認証した上でアクセスを許可するため、マルウェアなどの脅威が発生する可能性を低減することができます。
UEBA（ユーザーエンティティの行動分析）	分析データを活用して、セキュリティリスクを軽減し、異常を検出、ユーザーエクスペリエンスの最適化、モバイルワークへの適応を実現します。
Lookout CASBおよびSWGとの統合	Lookout Cloud Access BrokerでSaaSアプリケーションを識別、分析、保護し、Lookout Secure Web Gatewayでインターネットアプリケーションまで保護領域を拡張 します。
DLP（高度なデータ損失防止）	機密データの漏洩をリアルタイムで検知・停止し、データ保護ポリシーを実行してプライバシー規制の遵守を徹底します。
E-DRM（エンタープライズデジタル著作権管理	機密性の高い社内文書を分類し、通信中および保存されたデータの暗号化を実施することで、許可されたユーザーのみが機密ファイルにアクセスできるようにします。
Optical Character Recognition（OCR）と Exact Data Matching (EDM)	機密文書や機密キーフレーズをリアルタイムで特定・保護し、事故または悪意のあるデータ流出を防止します。
マルウェア検知、行動分析、インシデント対応	SaaSやインターネットアプリケーションのインバウンド/アウトバウンドのトラフィックをスキャンしてウイルス、マルウェア、ランサムウェアを隔離し、リスクの高い行動パターンを特定してインシデント対応を自動化することで、攻撃を阻止してユーザーとリソースを保護します。

ivanti

ivanti.co.jp
03-6432-4180
contact@ivanti.co.jp