

# NetWitness® SASEと統合

## 比類のないネットワーク完全可視化



従業員の働く場所がますます分散化しており、このトレンドをサポートする新しいテクノロジーが必要とされています。セキュア・アクセス・サービス・エッジ（SASE）とクラウド移行は、コスト削減と効率化をもたらしますが、暗号化されたトラフィック、リモートユーザー、クラウドワークロードの可視化など、新たなセキュリティ上の課題をもたらします。攻撃対象領域全体を完全に可視化することが重要です。

### 死角をなくす SASEのセキュリティを強化

NetWitnessは、主要なSASEベンダーと提携し、必要に応じて暗号化されたデータも可視化する技術的な統合を行うことで、この問題に対処しています。これは、SASEのユースケースだけでなく、オンプレミスとクラウドのデータを横断的に監視するという極めて重要なハイブリッドのユースケースもサポートします。お客様は、SASEの柔軟性とSASEが本来持つセキュリティ上の優位性、そして完全な脅威検知と対応の可視性という、両方の長所を享受することができます。

### スケーラブルで高性能なクラウドセキュリティ

- i 企業全体にわたる完全なネットワークの可視化と脅威の検知を実現し、もはや制御できない部分まで検知します。
- i ルール、パーサー、フィード、機械学習など、使い慣れたオンプレミスのメカニズムを使用して、すべてのリモートユーザーのネットワークトラフィックを検出および分析します
- i 単一のユーザーインターフェイスにログインして検索やその他のインタラクションを実行し、発信元を問わずネットワーク通信の結果を迅速に受け取ります。
- i 検知をトリガーにフォレンジック調査を行い、保持されているネットワーク通信に対し未知の脅威がないか脅威ハンティングを実行します。

### 主な機能

- すべてのリモートユーザーのネットワークトラフィックをほぼリアルタイムでキャプチャ
- コンポーネントはハイブリッド、オンプレミス、クラウドのいずれでも可能
- どこから収集されたデータであってもすべて、検出エンジンにアクセス可能で、アナリストのインタラクションに利用できる
- デプロイメントがカスタマイズ可能なので、個人を特定できる情報（PII）を保存するリスクを制限

## 一つのソリューションとして機能する

NetWitnessのSASE統合により、企業はクラウドセキュリティスタックを完全に可視化できるため、クラウドトラフィックの盲点をコスト効率よく排除し、セキュリティインフラストラクチャへの投資効果を最大限に高めることができます。企業は、オンプレミスかクラウドかを問わず、暗号化されたトラフィックを可視化し、制御することで、プライバシー、規制、および許容される使用ポリシーへのコンプライアンスを確保できます。

単一ユーザーインターフェイス	NetWitnessとSASEの統合構造は、オンプレミスとクラウドのハイブリッドシナリオをサポートし、データの収集場所に関係なくデータを分析できます。アナリストは、単一のユーザーインターフェイスにログインして、インデックス検索、メタデータを介したピボット、ネットワークセッションの再構築を実行し、迅速に結果を得ることができます。
生のネットワーク通信を保持	検知をトリガーに保持されているネットワーク通信に対し未知の脅威がないかアナリストがフォレンジック調査および脅威ハントを実行できるようにします。リモートユーザーの接続先ネットワークのパケットはすべて保持されます。
異なるデータセットの相関	アナリストは、リモートアクセスユーザーの実際のネットワークトラフィックから検出された情報を、同じユーザーによる他のアクセスと関連付けることで、調査のコンテキストを充実させ、何が起こったかをエンドツーエンドで完全に把握することができます。
ストレージ最適化	NetWitnessは、新しい圧縮アルゴリズム、選択的なリテンション、ネットワークデコーダーコンポーネントの分割を使用して、クラウドで実行するものを制限することにより、顧客の運用コストを最小限に抑えるよう努めています。

## NetWitnessプロフェッショナルサービス - お客様の成功のために

NetWitnessは、セキュリティ運用チームの継続的な成功を支援するサービスを提供しています。これらのサービスは、SOCの設計、実装、トレーニングから、マネージド検出および対応（MDR）、重大インシデント対応（IR）まで多岐にわたります。IRリテナーサービスは、大規模な攻撃や侵害が発生した場合の迅速な対応を保証します。

NetWitnessのSASEの統合により、お客様は両方のメリットを享受できます。  
SASEの柔軟性とセキュリティの優位性、そしてNetWitnessの脅威の完全な  
検出と対応の可視性。



詳細は<https://www.netwitness.com/ja/> をご覧ください。