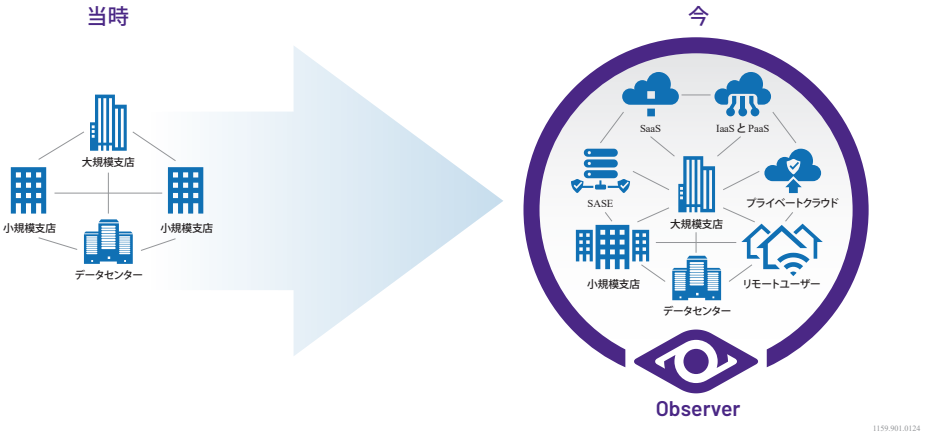
Observer Apex

NetSecOps のために構築：もっと見る。より速く解決する。
高度な分析を通じて包括的なネットワークとセキュリティの可視性を提供。

ネットワークはいたるところに

オンプレミス、または SaaS、IaaS、PaaS、SASE などクラウドベースのリソースでホストされる複雑な多層アプリケーション。ユーザーがどこからでもアプリにアクセスすることは、新しい規範となっています。今日のネットワークには境界はありませんが、各 IT サービスは依然として境界に依存しています。

ネットワークまたはサービスアーキテクチャのコンポーネントが劣化すると、アプリの配信の質が急速に低下し、顧客満足度および事業収益性の低下につながる可能性があります。これを回避するには、包括的なサービスの可観測性が必須となります。



Observer Apex は、最も必要な場所に可視性を提供し、すべてのトランザクションでエンドユーザー体験 (EUE) スコアを生成する初のパフォーマンス管理ソリューションです。Apex は、パケット、メタデータ、強化されたフローなど複数データソースを介して適応性と可視性を提供します。組織は予算に最適なソースを選択できます。

Apex は、包括的な可視性を提供するという同社の取り組みに沿って、グローバルな IT サービスの健全性とステータスを認識できるようにします。サービスの異常や潜在的なセキュリティ侵害が検知されると、効率的なワークフローにより、NetOps、DevOps、および SecOps グループが根本原因を突き止めて迅速に修理できるようします。

NETSECOPS のコマンドセンター

- 機械学習を利用した自動 EUE スコアリングは、複数の KPI を単一の理解しやすいメトリックスに変換し、詳細なスコア控除と組み合わせて問題領域を自動的に分離し、迅速な修復に優先順位を付けるために必要な情報を提供します。
- パケット、メタデータ、強化されたフローなどの柔軟なデータソースオプションにより、ネットワークエンジニアから事業部門責任者まですべての利害関係者に適切なビューが提供されます。
- 効率的なワークフローを備えたグローバル運用インテリジェンス用のカスタマイズ可能なダッシュボードにより、NetOps、SecOps、DevOps が問題を迅速に特定して解決できるようにする
- オンデマンドアプリケーション依存関係マッピングにより、設定を必要とせずに、高速かつ正確な多層アプリケーションの可視化が可能になります。
- サービス異常やサイバーセキュリティ侵害に迅速に対応できるように統合されたパフォーマンス管理とフォレンジック

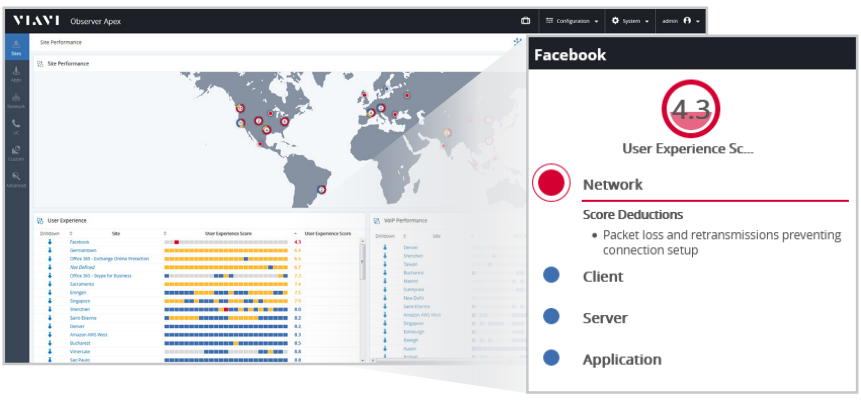
- ディープパケットインスペクション(DPI)機能は、ネットワークトラフィックの構成を理解し、重要でないトラフィックが主要なビジネスサービスやエンドユーザーに悪影響を及ぼしているかどうかを判断するという課題に対処します。
- CrowdStrike® が提供する脅威インテリジェンスを搭載した Observer 脅威フォレンジックは、パケットレベルの知見と組み込まれた敵対的なコンテキストを組み合わせて調査を強化し、ハイブリッド環境全体にわたって迅速なトリアージ、信頼性の高い検証、実用的な脅威の可視性をサポートします。
- デジタル証明書分析により、有効期限が切れた証明書や有効期限が近づいている証明書を特定し、古くなったプロトコルを強調表示して、コンプライアンスとユーザーへの中断のないサービスを共に確保します。
- 統一コミュニケーションワークフローは、グローバルサマリーやサイト固有ビューからインタラクティブ通話の詳細まで、UC エキスパートをガイドします。パケットデータとフローデータはシームレスに統合され、ネットワークインフラを介した単一のポイントツーポイントまたは複雑なマルチポイント通話のパスを可視化します。
- クラウドフローログの取り込みと分析により、クラウドトラフィックに必要な可視性が提供され、Amazon Web Services(AWS)や Microsoft Azure などのクラウド環境のセキュリティ脅威の検出、異常の特定、コンプライアンスの順守に役立ちます。
- データセンター専用アプライアンスから、シンプルで効率的なクラウド展開のための仮想マシンイメージまでの柔軟な展開オプション

パフォーマンス管理

エンドユーザー体験スコアリング

Apex は、機械学習を活用した特許取得済みの分析により、ユーザーの満足度の評価から当て推量をなくし、すべての会話を正確に分析し評価します。それぞれが 0 から 10 の間でスコア付けされ、色分けとグレーディングを使用してユーザーの観点からパフォーマンスを表示し、独自の環境とアプリケーションの動作を考慮して誤検知をなくします。

スコアは、単一ユーザーの体験を可視化するものですが、サイト、サービス、またはグローバルなエンタープライズビューに拡張することもできます。Apex は、わかりやすい問題の説明を使用して、問題をネットワーク、クライアント、サーバー、またはアプリケーションドメインに切り分けることで、これをさらに一歩進めます。



8〜10 = 良好(Good)

5.1〜7.9 = 軽度な問題(Marginal)

0〜5 = 重度な問題(Critical)

カスタム化した事業レベルのダッシュボード

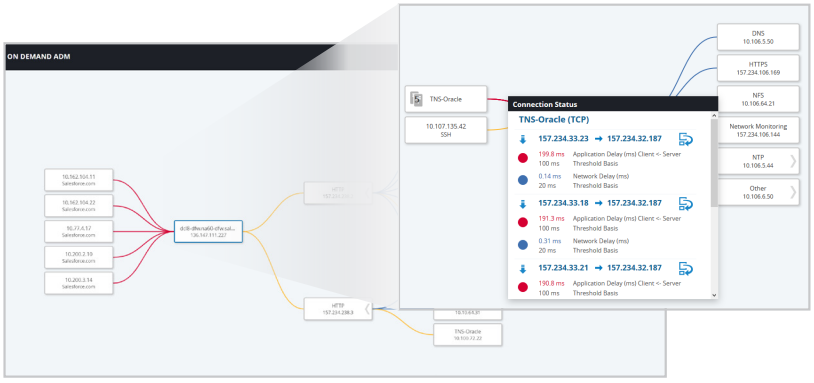
位置情報ベースのユーザー定義ダッシュボードにより、サービス提供の健全性に対する統合された企業全体の状況認識を可能にします。

トラブルシューティングのワークフロー

エンドユーザー体験スコアリングと統合されたサイトおよびサービス主導のワークフローにより、IT チームはすべてのリソースの世界規模の状況を即座に認識し、個々のユーザーにすばやく掘り下げて問題を迅速に解決できます。

オンデマンドの多層アプリケーションインテリジェンス

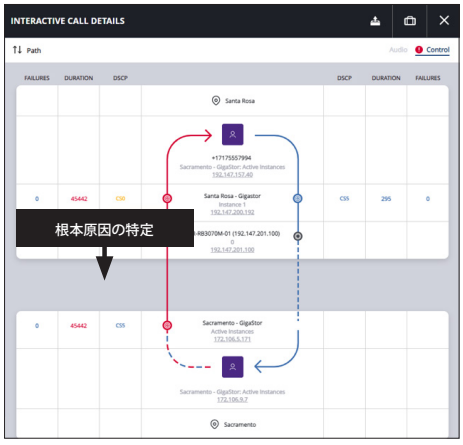
オンデマンドのアプリケーション依存関係マッピングは、多層サービスの認識、アプリケーションの相互依存関係の迅速な検出、およびこれらの複雑な関係を明確に可視化するマップのアドホックなレンダリングを提供します。Apex は、マウスのワンクリックでマップ全体を生成し、最悪の接続を自動的に特定して強調表示するため、ユーザーはトラブルシューティングの優先順位をすばやく割り当てることができます。



統合されたエンドユーザー体験スコアリングを備えた自動化されたアプリケーション依存関係マップ

ユニファイドコミュニケーション

Apex UC ダッシュボードとワークフローは、VoIP および UC エキスパートを、グローバルな概要やサイト固有のビューから、通話の詳細のユニークでインタラクティブな可視化まで効率的にガイドします。Observer だけが、パケットデータとフローデータをシームレスに組み合わせて、ネットワーク インフラを通る単一のポイントツーポイントまたは複雑なマルチポイント通話のパスを可視化し、必要に応じて関連するパケットデータにワンクリックでアクセスできるようにすると同時に、品質低下の根本原因を特定します。



インタラクティブな通話の詳細から品質低下の根本原因を特定します。

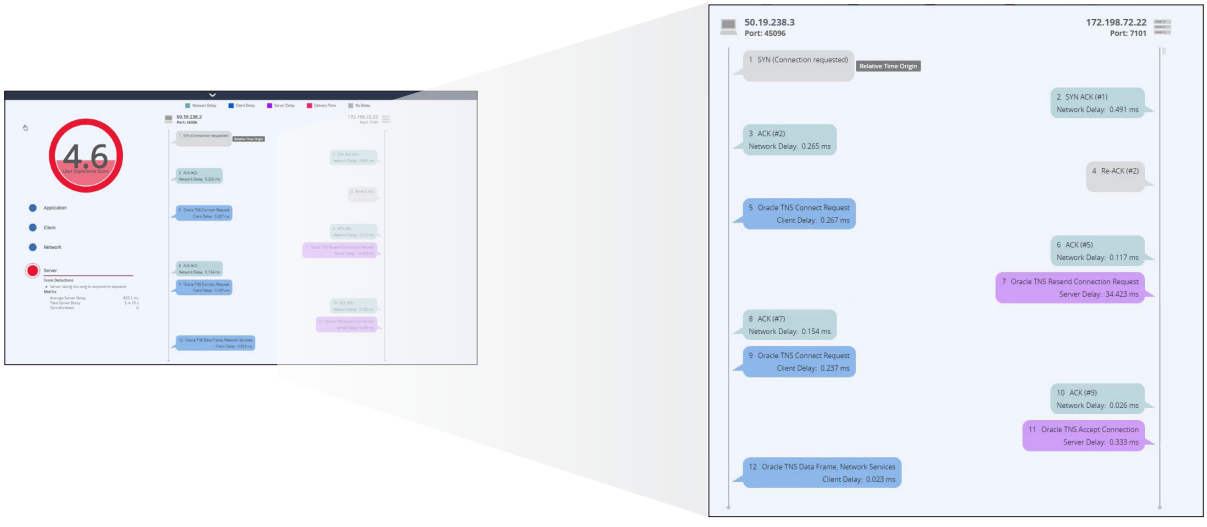
主な利点は次のとおりです。

- **ビジュアルジャーニーマッピング：**パケットとフローのデータをコールジャーニー用の直感的な可視化に変換
- **迅速な問題解決：**UC のパフォーマンス問題の根本原因を簡単に特定することで MTTR を大幅に削減
- **ユーザーフレンドリーなインターフェイス：**複雑なマルチポイントおよびポイントツーポイントの UC 通話を簡略化して表示することで、エキスパートでないユーザーでもサポートできるようにする使いやすく理解しやすいインターフェイス

ネットワークとセキュリティフォレンジック

Observer のネットワークフォレンジックは、データを長期間保持する機能を備え、パケットと強化されたフローの 2 つの補完的なデータソースを統合します。仮想マシンの画像展開オプションにより、クラウドでホストされるアプリの強化されたフローとパケットの収集と分析が可能になります。多くのパフォーマンスの問題やほとんどのサイバーセキュリティ侵害の根本原因の究明は、メタデータと直感的なダッシュボードから始まりますが、多くの場合、内在するデータの可視性につながる論理的ワークフローで終了し、時にはイベントの数日後になることがあります。そのため、Observer は長期間にわたって詳細をサポートし続けます。

前述のように、パフォーマンスの異常の多くは、エンドユーザー体験スコアリングによって迅速に分離されます。ただし、より忠実度の高い詳細が必要な場合は、サポートデータはすぐに利用可能になります。



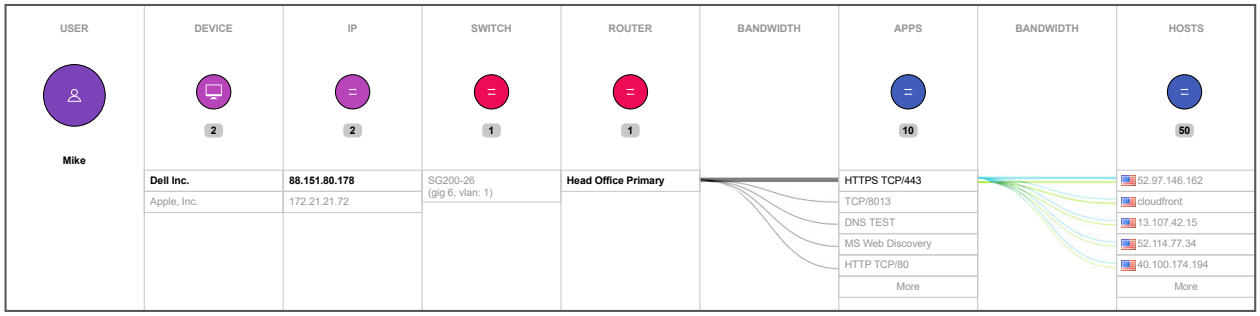
関連する接続の動的な会話のブレイクアウトによるエンドユーザー体験スコア

会話フォレンジック

Observer によってキャプチャされたパケットデータを使用すると、最初から最後までのすべてのトランザクションをレビューおよび調査アクションに利用できます。効率的なワークフローにより、ユーザーは必要に応じて、わずか数ステップでグローバルダッシュボードから個々のパケットに移動できます。

DPI 駆動のアプリケーション識別機能によって追加された可視性により、Observer は高度なネットワークトラフィックの知見を提供します。この機能により、ネットワークエンジニアは、非標準ポートで実行されているトラフィックを容易に特定し、重要ではないトラフィックを定量化し、HTTP や HTTPS などのプロトコルを詳しく調べることができます。Observer の DPI 機能により、4,300 を超えるアプリケーションを識別できるようになり、会話がビジネストランザクションなのか、それとも他のものなのかが一目で明確になります。

強化されたフローのフォレンジック



各会話ごとのネットワークインフラ全体にわたるユーザーアクティビティの
Observer GigaFlow IP ビューアーによる可視化

レイヤー 2〜レイヤー 3 の知見を 1 つの強化されたフローレコードにコンパイルすることにより、Observer は、ユーザー、IP アドレス、MAC アドレス、およびネットワーク全体のアプリケーションの使用状況間の関係を独自のインタラクティブな可視化で表します。ユーザーは、名前/ユーザー ID または IP アドレスを入力するだけで、それに関連したすべてのデバイス、インターフェイス、およびアプリケーションをすぐに見つけることができます。何が接続されていて、誰がネットワークを介して通信しているかを見つけることが、これまでになく容易になりました。

デジタル証明書の管理

Observer は、ネットワークトラフィックを分析しながら SSL/TLS ハンドシェイクを監視し、期限切れまたは期限切れに近づいているデジタル証明書を特定し、プロアクティブな通知を提供します。安全でないセッションを公開しているサーバーを特定し、古くなったプロトコルを強調表示し、コンプライアンスを検証し、ユーザーに対して中断のないサービスを確保できるようにします。

証明書分析ダッシュボードには、TLS バージョン、証明書の有効期限ステータス、および暗号スイートの配布が表示されます。

ネットワークエンジニアと管理者にとって、稼働時間と顧客満足度を確保することは、ウェブベースのサービス提供に不可欠です。スプレッドシートなどの手作業のレポート方法からプロアクティブな証明書分析アプローチに移行することで、プロセスが簡素化され、潜在的な証明書関連の機能停止から会社を守ります。

主な利点は次のとおりです。

プロアクティブな監視：リアルタイム分析、レポート作成、通知により、証明書の有効期限切れを事前に把握できます。

強化されたセキュリティに関する知見：運用中の SSL または TLS バージョンを明確に把握し、古いプロトコルや安全でないプロトコルを迅速に廃止することが可能

中断のないサービス：証明書関連の問題を特定して修正することで、潜在的な機能停止が回避し、シームレスなユーザー体験を保証します。

サイバーセキュリティに関して言えば、脅威に対する最善の保護には、予防、検知、対応の 3 つの側面からなる戦略が必要です。

防止		検知	対応
• ファイアウォール • DDoS 防止 • データ損失防止 • 侵入防止 • ウイルス対策とマルウェア	• 暗号化 • アンチスパム/フィッシング • アクセス制御 • エンドポイントセキュリティ	• 侵入検知 • セキュリティイベント管理（SIEM） • エンドポイント検出	• ネットワークフォレンジック • セキュリティイベント管理（SIEM）

多くの組織では、侵害が確認され、緊急作戦シナリオにより脅威への対応を開始するまで、多くの場合、予防と検知に重点が置かれます。この時点で、現在から過去に遡ってすべてのネットワークアクティビティにアクセスできるようにしておくことが、被害を抑え、自信を持って「警報解除」を宣言するために重要です。

ネットワークフォレンジックの価値がここで最大限に発揮されます。Observer は、トラフィックと強化されたフローのフォレンジックを組み合わせたパワーを提供し、すべてのサイバーセキュリティ侵害の、「どのようにして/誰が/何を/どこで」に答えることにより、ビジネスを再開できるようにします。

トラフィックのフォレンジック

デバイスはどのように接続されているか、または接続されていたか？

誰が通信しているか、または通信していたか？

強化されたフローのフォレンジック

何が送信されているか、または送信されたか？

疑わしい行動はどこまで広がったか？

これらの質問に答えることで、IT チームは「攻撃ベクトル」（攻撃者がどのように防御および検出手段を回避して侵入したか）と、どの IT サービス、デバイス、または機密の顧客/ビジネスのデータが不正アクセスされたかを迅速に判定できます。これが完了すると、封じ込めが可能になり、損害評価がまとまります。

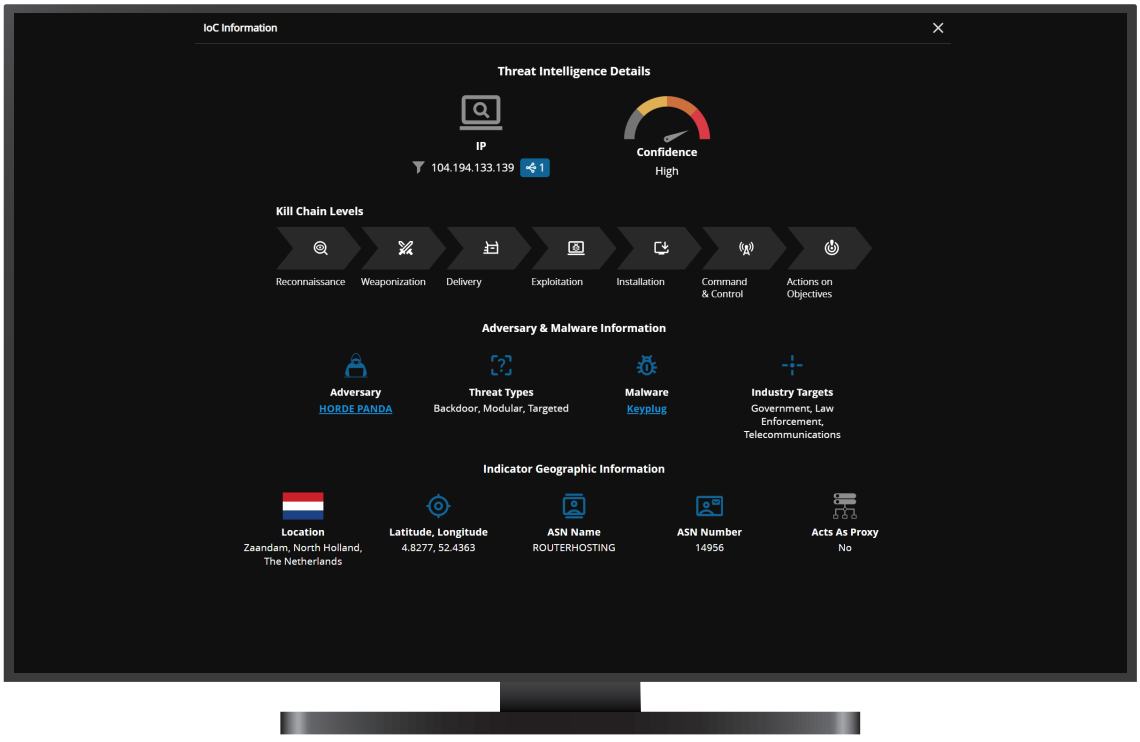
OBSERVER 脅威フォレンジック

確実な対応のための実用的な脅威の可視化

Observer 脅威フォレンジックは、CrowdStrike® が提供する継続的に更新される脅威インテリジェンスにより、エンリッチ化したフローとパケットレイヤーの証拠を注入し、ネットワークフォレンジックに新たな次元を追加します。これにより、セキュリティチームは、敵対的な挙動と疑わしいトラフィックパターンおよびパフォーマンス低下をすべてリアルタイムで関連付けることができます。

Observer は、侵害の兆候（IOC）、攻撃者の TTP、その他の敵対的な詳細を検出した瞬間に組み込むことにより、手動でステッチしたり、エンリッチ化を遅らせたりすることなく、即座に信頼性の高い脅威の検証を可能にします。

既知の脅威またはネットワークトラフィックパターンの予期しない挙動のいずれがトリガーであっても、各アラートには、生のパケットデータとエンリッチ化されたフローメタデータへのピボットレディアクセスが含まれており、アナリストは、ハイブリッド環境全体で、影響の評価、範囲の調査、根本原因の特定、および決定的なアクションを取るために必要な証拠を得ることができます。



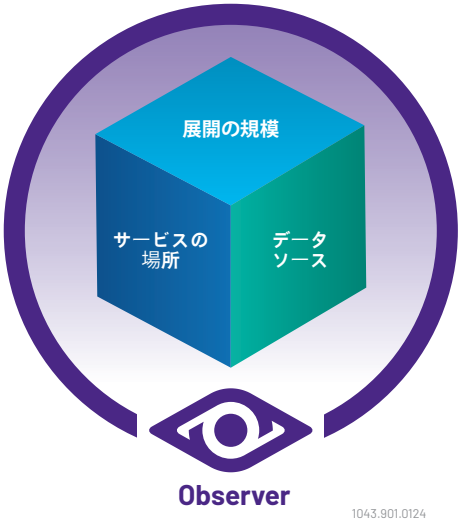
通常、初日から開始する従来のソリューションとは異なり、Observer 脅威フォレンジックは真のレトロスペクティブ解析を可能にし、セキュリティチームが脅威をゼロ日目まで遡ることができるようにします。長期間にわたって保持される完全に忠実なデータにより、最初の検出前であっても、アナリストは攻撃のタイムラインを完全に再構築し、根本原因、エントリポイント、ラテラルムーブメントを信頼できる唯一の情報源内で明らかにすることができます。

主な利点は次のとおりです。

- **ネットワークトラフィックと脅威インテリジェンス間のリアルタイムの相関**により平均修復時間（MTTR）の短縮と当て推量の削減を実現
- **レトロスペクティブ解析**はゼロ日目の可視性を提供することで、セキュリティアナリストが最初の検出前の脅威活動を調査するために必要なフォレンジック証拠を提供
- **組み込まれた攻撃者コンテキスト**と TTP が確実なトリアージと調査をサポート
- **パケット証拠への直接リンク**により範囲と影響評価の迅速な詳細分析が可能
- **可視性の共有**により NetOps と SecOps のワークフロー全体でのコラボレーションを推進

Observer 脅威フォレンジックは、パフォーマンスと脅威活動を相関させる共有された忠実度の高い全体像によりネットワークとセキュリティの運用を統合することで、調査を強化し、ワークフロー全体の信頼性を向上させます。統合されエンリッチ化されたフローとメタデータにより、リアルタイムのトリアージと侵害後のフォレンジックに必要な粒度と保持を提供し、当て推量を排除して解決を加速します。

OBSERVER の概要

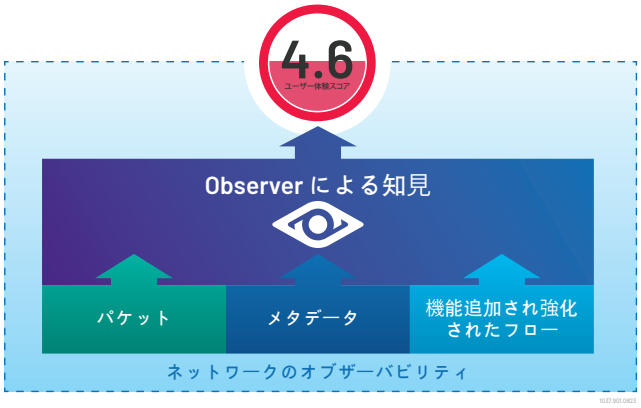


VIAVI Observer プラットフォームは包括的なパフォーマンスおよびセキュリティ管理ソリューションで、ネットワーク、運用、セキュリティの各チームに、ハイブリッド環境全体にわたる実用的な知見を提供します。Observer Apex は、EUE スコアの計算のために複数のデータソースからトランザクションメタデータを収集します。フォレンジックレベルの脅威検出と調査を統合し、NetOps チームと SecOps チームに共有された可視性と信頼できる唯一の情報源を提供します。

統合ダッシュボードおよびレポート作成用リソースとして、Apex は、中央のグローバルな可視化ポイントとして、またパケット、メタデータ、および強化され機能追加されたフローを使用して根本原因を特定するのに役立つ最適化されたワークフローによる迅速なトラブルシューティングの起点として機能します。組み込まれた脅威コンテキストとフォレンジックデータへの直接アクセスにより、セキュリティチームはインシデントを検証し、影響を評価して根本原因を迅速に特定することができます。

Observer は、次の 3 つの主要な方法で IT チームを支援します。

- **サービスの場所** - Observer は、プライベートクラウド、リモートユーザー、支店やデータセンターのオンプレミスなど、あらゆるホスティング環境への可観測性を提供します。場所がどこであれ、VIAVI Observer が対応します。
- **データソース** - Observer は、パケット、エンリッチ化されたフロー、メタデータを使用して柔軟な可視化オプションを提供します。この多層的なアプローチは、パフォーマンスのトラブルシューティングと侵害後のフォレンジックの両方に対応します。役割ベースのワークフローとコンテキスト豊富なアラートにより、チームは適切なタイミングで適切なデータを使用し、サービスの異常からセキュリティの脅威まで、自信を持って調査することができます。
- **展開の規模** - 小規模で開始し、運用とセキュリティ需要の進化に合わせて規模を拡大可能 VIAVI は、お客様の OpEx または CapEx のニーズに合わせて、柔軟な導入モデルと段階的なサブスクリプション価格を提供し、予算やリソースを過度に増やすことなく、スケーラブルな可視化と NetSecOps コンバージェンスを可能にします。



詳細については、viavisolutions.jp/apex をご覧ください。

viavisolutions.jp

〒163-1107
東京都新宿区西新宿6-22-1
新宿スクエアタワー7F

電 話：03-5339-6886
FAX: 03-5339-6889
Email: support.japan@viavisolutions.com

apex-br-ec-ja
30193606 914 1025