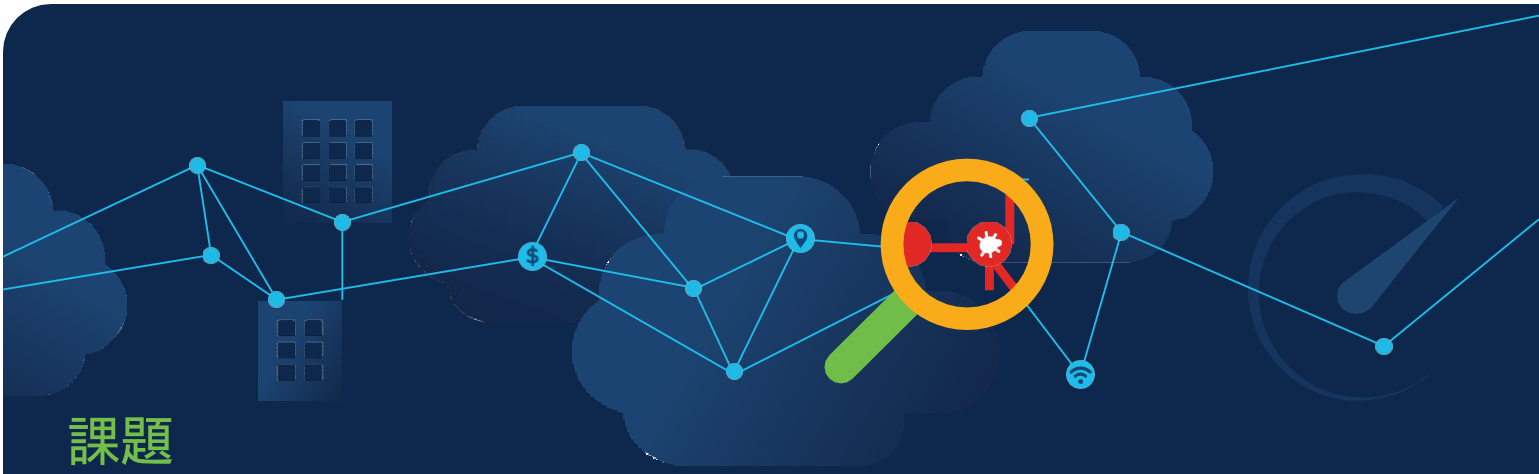
可視化とセキュリティ分析によりネットワークでゼロトラストを確立

Cisco Stealthwatch の継続的なネットワークトラフィック監視能力により、悪意の兆候を検出してポリシーを動的に適用する



課題

ゼロトラストがなぜ必要なのでしょうか？その理由は、ネットワークの複雑化や脅威の進化といった、今日の企業が直面している課題にあります。まずクラウドへの移行により、あらゆる場所やデバイスからネットワークにアクセスするユーザが増えています。しかも暗号化されたトラフィックが増え、IoT が急増しているため、従来の「ネットワーク境界」という概念が崩れつつあります。それと同時に攻撃方法も進化しています。例えば侵入に脆弱性を利用することや、流出したログイン情報を利用することもあります。侵入後はデータを暗号化して盗み出す場合や、ネットワークに潜伏し続ける場合もあるなど、攻撃者は柔軟に手口を使い分けています。

ゼロトラストとは？

ゼロトラストは、現状を踏まえた現実的なセキュリティを構築するためのアプローチです。テクノロジーやツールではなく、セキュリティアーキテクチャと手法を指します。これらのアーキテクチャと手法は、テクノロジー、プラクティス、ポリシーが組み合わされた複雑な環境を管理するという、今日の難しい課題を念頭に置いています。従来のセキュリティアプローチから、ベンダーが異なる複数の製品やサービスを統合して相互運用性するソリューションアプローチへと進化したものだと言えます。

ゼロ トラスト アーキテクチャ フレームワークでは、システム、アプリケーション、データリソースへのアクセスを、それらが本当に必要な認証済みユーザやデバイスに制限します。アクセスを認めた後も、ユーザやデバイスの ID とセキュリティ態勢を継続的に確認することで、各リソースに対する適切な許可を確保しつつ、必要なアクセス制御を継続します。[1]

ゼロトラストネットワークにおける可視化とセキュリティ分析の役割

Forrester 社のレポートによれば、Zero Trust eXtended (ZTX) Ecosystem[2] の重要な一角を占めるのはネットワークです。ネットワークを保護するために欠かせない要素は可視性です。そのネットワークをゼロトラストで保護するために欠かせない要素は可視性です。そのためレポートでも、ネットワーク分析・可視化（NAV）ツールの重要性を強調しています。NAV は、ネットワークトラフィック分析（NTA）またはネットワーク検出・応答（NDR）としても知られており、ネットワークトラフィックを直接分析することで脅威を幅広く検出し、迅速な対応を可能にします。

NAV の代表格が Cisco Stealthwatch です。ネットワークテレメトリを収集することで、プライベートネットワークからパブリッククラウドに至るまで、企業全体を可視化できる稀有なソリューションです。Stealthwatch の強みは、振る舞いモデリングと機械学習により実現した高度なセキュリティ分析能力です。それにより最新の脅威をリアルタイムで検出してピンポイントで特定し、IT チームに警告します。手作業による介入を必要としない集約型ソリューションであり、暗号化されたトラフィックからも包括的に脅威を洗い出すことが可能です。

Stealthwatch の設計コンセプトは、ユーザやデバイスの場所を問わず、すべてのネットワークアクティビティが「正常」か継続的に監視し、異常があれば即座に検出することです。続くセクションでは、Stealthwatch によりネットワークでゼロトラストを確立するための実装について、さらに詳しく説明します。

コンテキストに応じたネットワーク全体の可視性

Stealthwatch は、ルータ、スイッチ、ファイアウォールなどのネットワークデバイスからテレメトリを取り込んで分析します。パブリッククラウドインフラからテレメトリを収集する能力もネイティブで実装しています。サーバやプリンタなどのネットワーク接続機器やエンティティに対しては、**エンティティモデリング**により分類することで、各エンティティの正常な振る舞いを正確なベースラインとして把握し、異常があれば警告します。Stealthwatch の別の独自機能は、ネットワークの非対称パスを流れるトラフィックフローを統合し、クライアントとサーバ間の通信を再現できることです。つまり脅威を検出するだけでなく、脅威の発生元に関する**詳細情報**（脅威の拡大が疑われる横方向の場所、侵害されたユーザ、場所、デバイスタイプ、タイムスタンプなど）を提供できるのです。これらのテレメトリは一定期間にわたって保存されるため、過去や長期のイベント調査でも大きな役割を担います。ネットワークテレメトリだけでなく、他のソリューションから提供されるユーザ / アプリケーションデータや Web 情報などを Stealthwatch 上で統合して、脅威の調査と対応をさらにスピードアップすることもできます。

予測脅威分析

攻撃者による侵入経路は無数考えられるため、「盾」となる防御手段が少なくては防ぎきれません。そこで Stealthwatch は 3 つのアプローチを採用することで、高度な脅威に対しても鉄壁の防御で防ぎます。

- 最初のアプローチは**振る舞いモデリング**です。振る舞いモデリングはネットワークアクティビティを常時観察し、正常な振る舞いのベースラインを確定させます。そこに 100 種近くのヒューリスティックを使うことで、異常をすぐに警告できます。もちろん、従来からある不正操作についての蓄積されたデータも備えています。流出したログイン情報を使用して攻撃者が侵入した場合や、機密データを従業員が不正に持ち出している場合などは、Stealthwatch が瞬時に検知します。**まさにこのため、適切なアクセス許可を付与した後であっても、ネットワークアクティビティを継続的に検証することが不可欠なのです。**
- 2 番目のアプローチは随所における**機械学習**の応用です。機械学習により膨大な量のテレメトリから異常だけを洗い出し、隙間のない脅威検出を実現します。これによりセキュリティチームは、脅威の調査という重要な業務に集中できます。Stealthwatch の機械学習エンジンはクラウドベースであり、世界中の不正なサーバとの通信を見逃しません。これにより未知の攻撃や標的型攻撃さえも検出します。
- そして 3 番目のアプローチは、業界トップクラスの Cisco Talos から提供される**世界的な脅威インテリジェンス**を活用することです。脅威がローカルで発見された場合、即座にグローバルの事例との関連性を特定し、同じマルウェアによる被害の拡大を阻止します。Stealthwatch では 3 つのアプローチが互いに連携することで、定期的な ping 送信やビーコン発信、ポートスキャン、不正ドメインへの通信といった侵害の兆候を、早期から特定します。

暗号化トラフィックの分析

暗号化トラフィックの急増により、脅威の状況が変化しています。暗号化される Web トラフィックの割合は今や 80%を超えています。これは組織にとって大きな死角となってきました。暗号化トラフィックに対して、現行ソリューションの大半は復号ベースの監視アプローチを採っています。しかしトラフィックの復号は多大な時間とリソースを必要とし、さらにデータのプライバシーとセキュリティを弱めています。

米国国立標準技術研究所（NIST）は最近、『SP 800-207: Zero Trust Architecture (ZTA)[3]』（SP 800-207：ゼロトラストアーキテクチャ（ZTA））の題名の草案で、ネットワークセキュリティに対する新アプローチの概要を発表しました。すべてのトラフィックを逃さず検査し、ログに記録して分析することでネットワーク攻撃を検知して対応することの重要性などが述べられています。しかし業務で生じるトラフィックの一部は、サードパーティ製のシステムやアプリケーションから暗号化されて送信されるため、検査が困難です。

そのような場合に対して NIST は、暗号化トラフィックからメタデータを収集して分析し、ネットワークに潜むマルウェアや攻撃者を検出するよう推奨しています。草案では同時に、機械学習を応用した暗号化トラフィックの分析に関するシスコの調査について、次のように言及しています（22 ページのセクション 5.4）。

> 「暗号化トラフィックからメタデータを収集して活用すれば、ネットワークに潜むマルウェアや攻撃者を検出できます。復号して検査できないトラフィックに対しては、機械学習技術が有効です。このタイプの機械学習を使えば、トラフィック全体から悪意のある部分を抜き出して対処できます」

同じ研究結果に基づいて開発されたのが、Stealthwatch の Cisco Encrypted Traffic Analytics（ETA）です。ETA により暗号化トラフィックからでも脅威を検出できるだけでなく、復号しないため安全性やプライバシーも維持できます。

セグメンテーションとポリシーベースのモニタリングを簡素化

組織内外で発生するすべてのトラフィックを Stealthwatch で可視化すれば、重要業務に一切干渉しない、スマートなポリシーを作成して適用できます。セキュリティアラートをカスタマイズし、違反が起きれば即座に通知することもできます。たとえば、機密性のあるデータサーバにゲストユーザがアクセスを試みた場合や、疑わしい国をトラフィックが経由した場合などです。これにより、他のツールで設定したセキュリティポリシーが実際に効果のあることを確認できます。Stealthwatch に統合された Cisco Identity Services Engine は、デバイスで脅威の兆候を発見すると、脅威の重大度に応じて適切なポリシーを適用し、問題を即座に封じ込めます。

シスコのゼロトラスト

シスコのゼロトラストは、ユーザ、デバイス、場所を問わず、あらゆるアプリケーションと環境をまたいでアクセスを全面的に保護するアプローチです。ワークフォース、ワークロード、および職場を保護します。

シスコは最近、『The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q4 2019』（The Forrester Wave：Zero Trust eXtended エコシステム プラットフォーム プロバイダ - 2019 年第4 四半期）でリーダーに選出されました。詳しくはこちらのレポートをご覧ください。

まとめ

ネットワークに誰が接続し、何をしているかを把握することは、不正操作を見逃さず瞬時に検出するために不可欠です。こうしたセキュリティ体制はゼロトラストの確立に欠かせません。そのために役立つのが、ネットワークテレメトリを収集して分析し、信頼性の高いアラートとして警告できる Cisco Stealthwatch です。追加のセンサーやプローブを導入することなく、規模を問わずシンプルに実装できることが特徴です。

次のステップ：

ネットワークでゼロトラストを確立するための取り組みを始めましょう。今すぐ 2 週間の可視性アセスメントを無料でお試しください。

Cisco Stealthwatch の詳細につきましては、https://www.cisco.com/c/ja_jp/products/security/stealthwatch/index.htmlをご覧ください。

出典：

1. ホワイトペーパー『Zero Trust 101』
2. Forrester 社：『The Zero Trust eXtended (ZTX) Ecosystem: Networks』
3. NIST 特別草案 800-207（第 2 版）：『Zero Trust Architecture』

2063648　04/20