ネットワークをセキュリティ センサー およびエンフォーサへ進化させて ビジネス セキュリティを強化する

2016 年 4 月

作成者:

Zeus Kerravala

ネットワークをセキュリティ センサーおよびエンフォーサへ進化させてビジネス セキュリティを強化する

ゼウス・ケラバラ著

2016 年 4 月

ZK Research
Kerravala Consulting
傘下の事業部門

概要：デジタル進化によって高まる普遍的なセキュリティの必要性

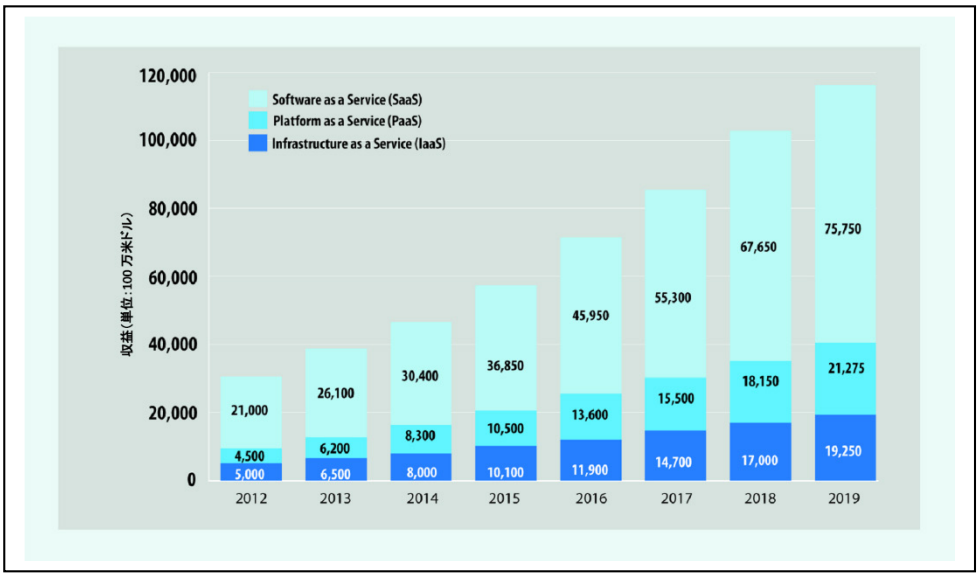
世の中のデジタル化が急速に進み、IT を取り巻く状況は新しいビジネス環境のニーズに合わせて進化しています。クライアント/サーバはクラウド、モバイル コンピューティング、Internet of Things（IoT）に取って代わられ、業界はサーバ セントリックからネットワーク セントリックへと軸足を移しています。すべてのビジネス システムは、共通ネットワークに結び付けられています。ネットワーク セントリック コンピューティングへの移行によって世界は小さくなり、企業はデジタル エコノミーを活用できるようになりましたが、次のような新たなセキュリティの問題も生み出しています。

- **明確に定義された企業の境界の消滅**：従来、企業の境界の保護は、1 つの入口のみが対象の単純な作業でした。クラウドが台頭した今、クラウドのパフォーマンスを向上させるためには、インターネットへの接続数を増加せざるをえません。クラウドが飛躍的に増加し続ける中（図 1）、境界の細分化が進み、脅威にさらされやすくなります。

zeus@zkresearch.com

ソーシャル メディアを通じて影響力と洞察力のある情報を提供

図 1：クラウドの増加につれて脅かされる IT セキュリティ



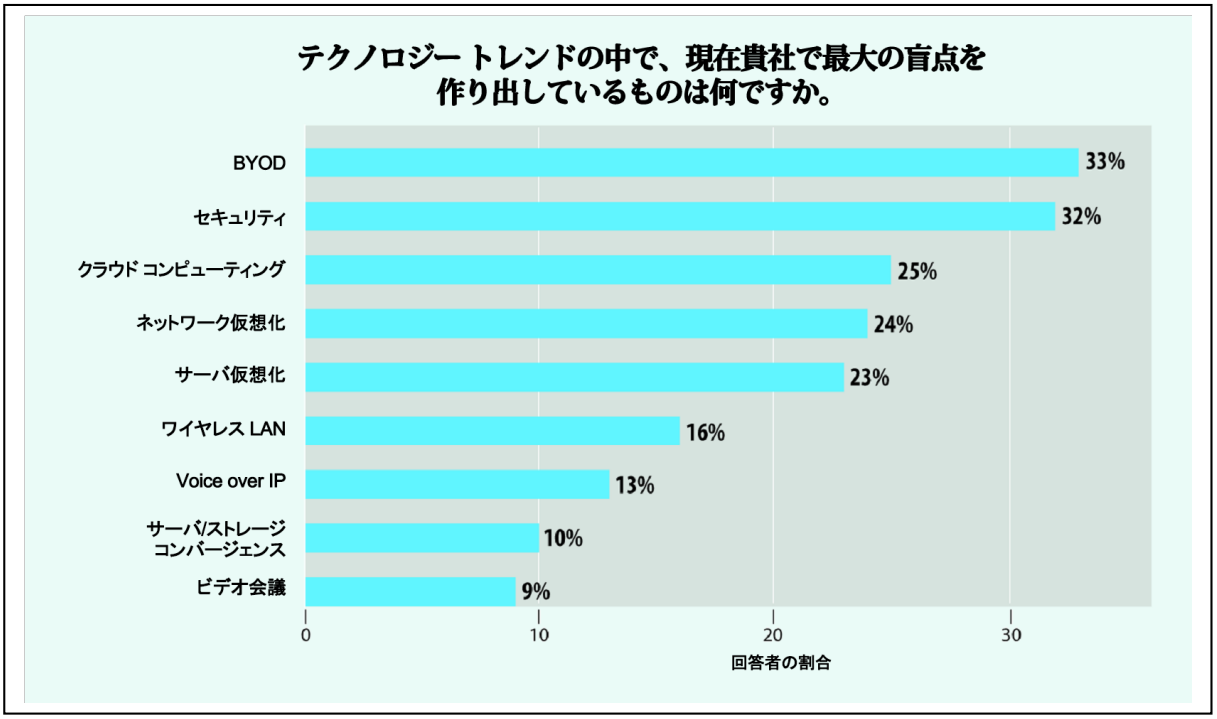
- **従来のエンドポイント セキュリティ戦略はもはや非効率**:エンドポイント セキュリティは長年にわたって、ほぼすべての企業におけるセキュリティ戦略の核心となっていました。このタイプのセキュリティは、IT 部門があらゆるデスクトップ、ラップトップ、モバイル デバイスを厳しく管理している場合には有効でした。しかし、ZK Research 2015 Network Purchase Intention Study の調査結果では、組織のほぼ 90 % が Bring Your Own Device(BYOD; 個人所有デバイス持ち込み)ポリシーを実施しており、個人デバイスの職場への持ち込みが許可されていることが示されています。このように、エンドポイントへの管理が低下したため、一貫性のあるエンドポイント ソリューションの維持がますます困難になりました。
- **シャドー IT が生み出す IT への多数の「盲点」**:Software as a Service(SaaS)ベースのアプリケーションが普及し、調達しやすいこともあって、基幹業務部門では IT またはセキュリティ担当者の手を借りずにアプリケーションを購入することが可能になりました。大企業の中には、基幹業務部門が直接購入したアプリケーション数が数百にも及ぶ例もあります。これらのアプリケーションは IT 部門が把握していないため、ビジネスとの間で送受信される情報のセキュリティ保護は、きわめて困難になります。

ビジネス ネットワークはもはや壁で囲まれたものではありません。企業ネットワークは、自宅、パートナー組織、カフェ、ホテルなど、企業データへのアクセスが必要な従業員が訪れる全ての場所にまで拡張されます。デジタル時代にあっては、速度が競争優位性を左右します。つまり、いつでも、どこでも、どのデバイスでも、データやその他のリソースにアクセスする必要があるということです。

BYOD のコンセプトが標準になると、企業にとって大きな「盲点」が作り出されます。実際、ZK Research 2015 Network Purchase Intention Study では、BYOD は現在の組織の最大の盲点としてランク付けされています(図 2)。

BYOD および IoT によって、さらなる複雑性も生じています。すなわち、接続されたデバイスの急増です。ZK Research では、接続されたデバイスの数は 2020 年までに 500 % 増加すると予測しています。つまり、組織の従業員数の増加がなくても、IT 部門は、現在と比較して 5 倍の接続エンドポイントをサポートしなければならないということになります。

図 2:BYOD は IT 部門にとって 1 番の盲点



こうした接続エンドポイントの急増とビジネス ネットワークの台頭とがあいまって、攻撃対象領域の数が増加し、攻撃の多くがモバイル デバイスを直接狙うようになりました。ZK Research 2015 Network Spending Survey では、組織の 74 % が、過去 12 ヵ月間でモバイル固有のマルウェアに対処したことがあると回答しています。

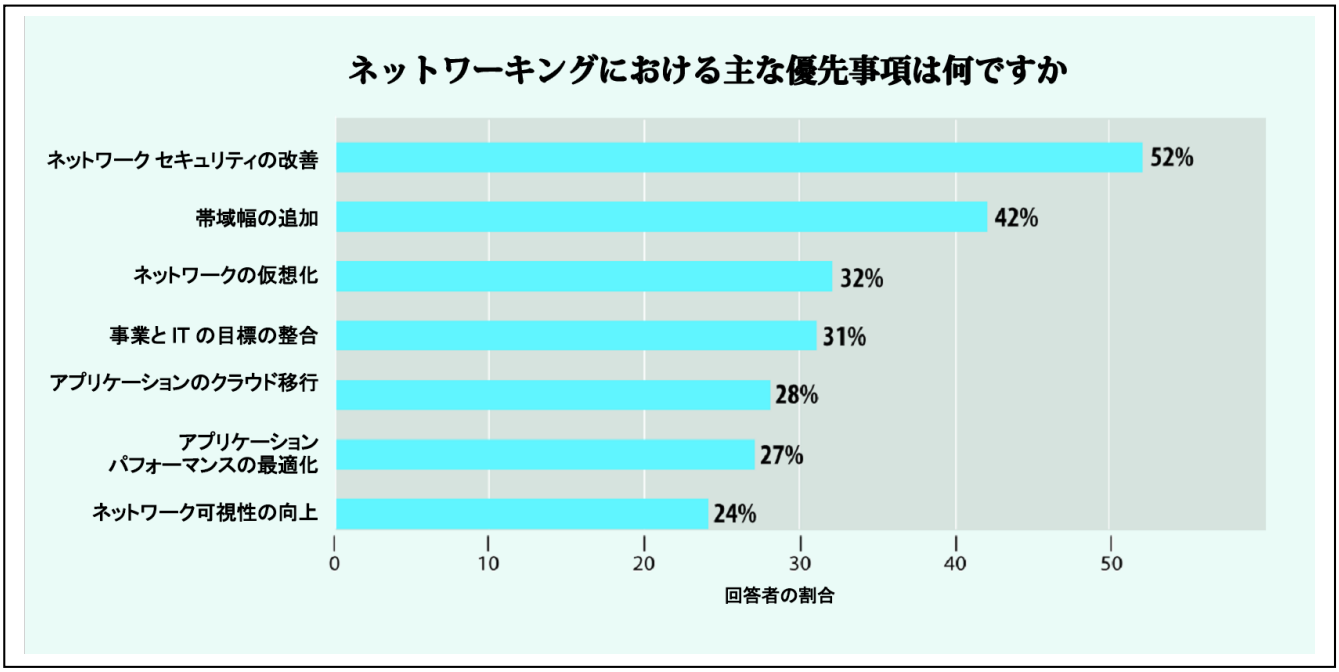
デジタル エコノミーや Internet of Everything（IoE）は企業とお客様に新たなチャンスを作り出すだけでなく、ハッカーや攻撃者にとっても新しいチャンスを作り出します。デバイスが増加するにつれ、悪用できる攻撃対象領域も拡大するためです。どのようなセキュリティ侵害であれ、組織には数百万ドルものコストが発生し、ブランドは著しく損なわれ、場合によっては訴訟のおそれもあります。ネットワークに接続される IT システムの増加を受けて、企業はセキュリティに対して脅威中心型のアプローチをとる必要があります。セキュリティをインフラストラクチャの中心に据えることで、デジタル変革の変化に対処できるのです。

デジタル化によって IT 環境はますます複雑になり、組織のセキュリティ保護が困難になっています。境界が崩壊した今、従来のセキュリティ手法にもはや効力はありません。セキュリティ プロフェッショナルは、ネットワークを保護し、侵害をできるだけ迅速に特定して修復するための手段としてネットワークを使用することに集中する必要があります。本書では、脅威を取り巻く状況の変化と、ネットワークをセキュリティ センサーおよびエンフォーサへと転換することでネットワーク セキュリティを強化する方法を紹介します。

セクション II：進化する脅威と拡大する攻撃対象領域

ビジネスのセキュリティ保護の複雑性は、高まるばかりです。その結果、ZK Research 2015 Network Purchase Intention Study によると、IT セキュリティ強化の必要性は、ネットワークの課題で第 1 位に挙げられています（図 3）。クラウド コンピューティング、仮想化、モバイル デバイス、Internet of Things が存在する中、攻撃対象領域は大幅に拡大しています。次のことを考えてみてください。ZK Research は、10 年前には 1 台であったユーザ 1 人あたりのデバイス数が、2015 年には 3.5 台に増加したと推定しています。これはデバイス増加の観点のみから見ても、攻撃対象領域の規模は 350 % 増加していることになります。そして、クラウド アプリケーションと Internet of Things の影響が加わった今、攻撃対象領域の数が 10 年前と比較して 10 倍になったと推定されても、驚くには値しません。

図 3：ネットワーク セキュリティの強化が最優先事項



出典：ZK Research 2015 Network Purchase Intention Study

また、脅威の検出も困難さを増しています。ZK Research の継続的な調査では、侵害の 80 % が境界ではなく企業内部において発生しており、個人デバイス上のマルウェアや、電子メールやフィッシング サイトをクリックしたことで感染していると推定されています。時にはマルウェアは数ヵ月間も休眠状態を維持し、攻撃を開始する前に情報を入手することもあります。

脅威中心型の状況に対処するべく、ZK Research 2015 Network Purchase Intention Study によると、企業では 12 ～ 30 社のセキュリティ プロバイダーからセキュリティ製品を導入しています。しかし、複数のセキュリティ製品の情報を関連付けることは非常に困難で、多数の盲点が発生する原因になります。現在、侵害の検出に手間取る主な原因は、この点にあります。セキュリティ違反の検出に時間がかかると、攻撃者がネットワーク上で情報を盗んだり邪魔されずに悪事を働いたりする時間が増えてしまいます。

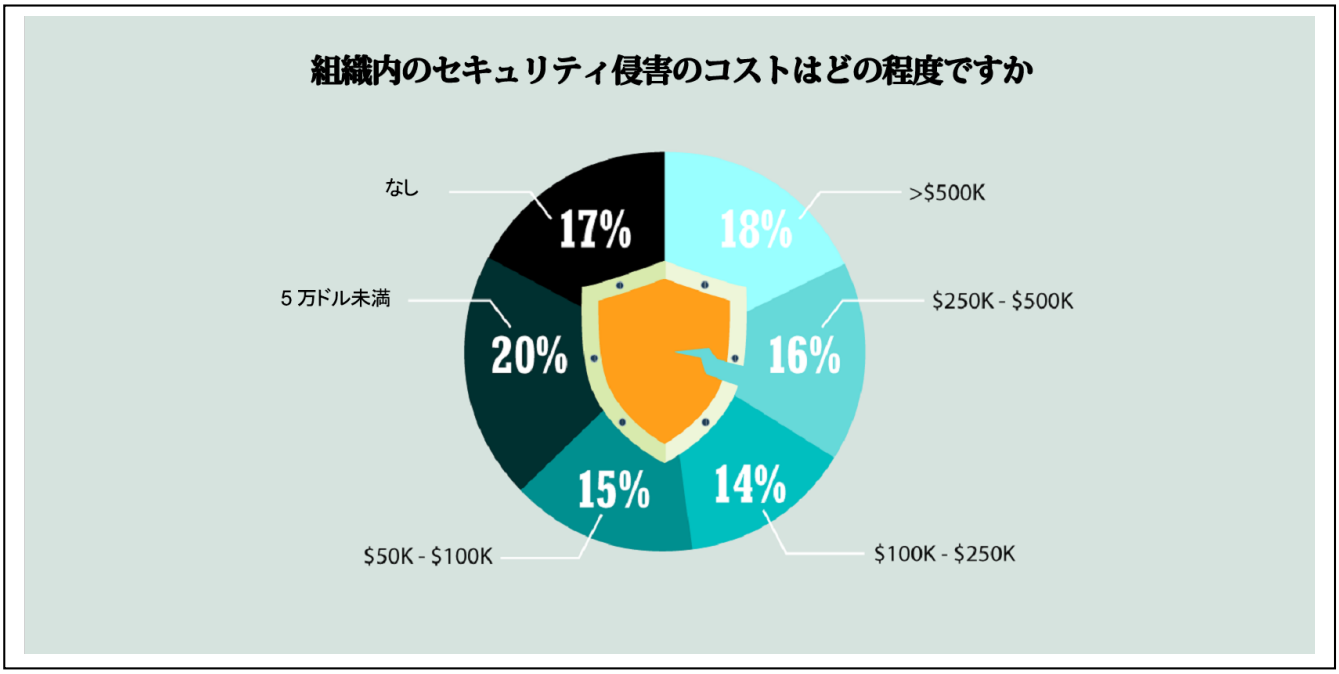
企業は組織の保護に文字通り数十億ドルもの資金を投入していますが、従来のセキュリティ製品は防止策または「特効薬」的なアプローチにしか目を向けておらず、これでは効果がありません。ZK Research は、企業の 85 % が過去 5 年間に攻撃を受けており、これらの攻撃は非常に高くつくと推測しています。ZK Research 2015 Security Study では、組織の 48 % が、1 件のモバイル インシデントが生むコストは 100,000 ドル以上であると回答しています（図 4）。

今こそ、テクノロジー リーダーおよびビジネス リーダーは、従来のエンドポイントまたはネットワーク セキュリティに関するこれまでの考え方を捨てて、脅威中心型の戦略に移行する時期です。それには、エンタープライズ ネットワークからデータセンター、IoT、クラウドおよびエンドポイントまで、ネットワーク全体でセキュリティを把握し、さまざまな攻撃ベクトルからの保護を実現し、新しいビジネス チャンスを獲得できる成長エンジンとしても活動する必要があります。

セクション III：シスコの脅威中心型アプローチによる、攻撃サイクル全体にわたる保護

企業を保護するには、まずネットワークに接続しているのが誰で何かを理解しなければなりません。ネットワーク内のユーザ、デバイス、アクティビティを完全に可視化することが、セキュリティにとって最重要です。すべてのネットワークへの可視性を取得してネットワーク トラフィック フローを理解することで、異常なトラフィック、ユーザ アクセス ポリシーの違反、不正アクセス ポイントなどの不明なネットワーク接続エンドポイントの発見を、より簡単に検出できるようになります。

図 4：高いコストがかかるモバイル インシデント



シスコは、企業のセキュアなネットワークの構築に必要な、データセンター、キャンパス、ブランチ スイッチ、ルータ、ワイヤレス アクセス ポイントおよびその他のインフラストラクチャからなる、多種多様なネットワーク ポートフォリオを提供しています。また、企業がセキュリティに対して脅威中心型アプローチを採用して攻撃サイクル全体を対象とする、セキュリティ ソリューションのポートフォリオも豊富に用意しています。ネットワーキングとセキュリティの両市場のリーダーであるシスコは、他にないレベルの可視性を提供する、独自の地位を確立しています。ネットワークをセンサーとして機能させて侵害をすばやく検出し、エンフォーサとして機能させて侵害をすばやく切り分けて、生じる損害を抑制します。

ネットワークをセキュリティ センサーに転換する

ユーザ トレーニングをどれだけ積んでも、セキュリティ テクノロジーをどれだけ注ぎ込んでも、攻撃の発生を防ぐことはできません。肝心なのは、脅威がネットワークに広範に拡散する前に、すばやく検出することです。ただし、あらゆる場所への可視性がなければ、環境の保護は不可能です。

データは数万台のデバイスを通じて組織内外のユーザに移動するため、トラフィック パターンは規則性がなく予測不可能なものになり、エンドツーエンドの可視性はさらに困難になっています。それでも、ネットワークをセキュリティ保護するには、疑わしいトラフィック フロー、ポリシー違反、侵害されたデバイスを環境から検出する機能が不可欠です。幸い、シスコのお客様はネットワークをセンサーに転換するテクノロジーをすでに保有している可能性があります。ただ機能を有効にするだけです。

シスコは、Flexible NetFlow と呼ばれる機能を IOS に提供しています。これはあらゆるネットワーク通信を「把握」する、強力で優れた情報源です。NetFlow はサポートされるルータとスイッチを通過するすべてのトラフィックを監視し、記録します。また、IP トラフィックを特徴付けて、ネットワーク フローの送信元と宛先を特定できます。さらに、アプリケーション トラフィックに時間を対応付ける情報を提供できます。NetFlow はネットワークのレコーダーとして機能し、誰がどのシステムにどれだけの時間アクセスしたかという情報を示します。

NetFlow の機能は、携帯通話の請求書に含まれるデータに例えることができます。誰（または何）が通話し、いつ通話があったか、通話時間の長さもわかります。これは発生した通話に関するメタデータですが、会話の内容は含まれていません。

Cisco IOS Flexible NetFlow はセキュリティに対する脅威をリアルタイムで特定するツールとして使用できます。異常なアクティビティを識別し、分析によって侵入の発生源を特定できるフォレンジック情報を提供します。NetFlow からのデータは、将来的にコンプライアンス目的や、ネットワーク自動化、分析に使用できます。

図 5 に、NetFlow がネットワークをセンサーに転換して、疑わしいアクティビティをすばやく特定する方法を示します。

NetFlow はサードパーティのセキュリティ ツールに付加価値を追加することもできます。たとえば、Lancope® StealthWatch® System は、NetFlow 情報を使用して脅威のアラートを提供できます。NetFlow およびその他のタイプのネットワーク テレメトリを分析することによって、Lancope の StealthWatch システムはコンテキスト認識型のセキュリティ分析を実現し、高度な持続的脅威（APT）や分散型サービス妨害（DDoS）からゼロデイ マルウェアや内部関係者による脅威に至る幅広い範囲の攻撃をすばやく検出します。

また、NetFlow データを Cisco Identity Services Engine と組み合わせると、フロー情報にコンテキストがさらに追加されるので、管理者はネットワーク情報だけでなく、コンテキスト データを利用して作業できます。たとえば、Lancope StealthWatch は、IP アドレス 192.168.1.2 のデバイスではなく、「Tom のコンピュータ」から疑わしいトラフィックが発生していると特定できるようになります。

NetFlow はスイッチおよび NetFlow Generation Appliance によって生成されますが、Nexus 1000V およびユニファイド コンピューティング システム（UCS）サーバ上で動作する仮想ネットワーク インターフェイス カード（NIC）からデータセンターまで拡張が可能です。この機能によって、データセンター内の仮想マシンにまで至る可視性が得られ、水平方向の仮想マシン間の通信を取得できるのです。

Lancope StealthWatch 搭載 Cisco IOS Flexible NetFlow の分析によって、管理者は、ネットワーク アクティビティのベースライン（すなわち「基準」）に対する可視性を取得し、このベースラインから逸脱してアラートをトリガーする疑わしいアクティビティの存在を把握します。ここで、アラートは IP アドレス情報しか提供しないため、原因の究明と問題の解決のどちらに時間を費やすかという問題に突き当たります。ネットワークに接続するデバイス数の増加によって、IP アドレスによる攻撃の特定には非常に時間がかかります。その時間の間に侵害によって発生する損害がどれほど大きいか、考えてみてください。

そこで登場するのが、Cisco Identity Services Engine（ISE）です。

図 5：NetFlow の役割

出典：ZK Research（2016 年）

Cisco ISE はビジネス コントロールとセキュアなネットワーク アクセスを促進します。ネットワークからコンテキスト データ（デバイス タイプやユーザ ID など）を収集して、ユーザの識別と分類の精度を向上し、ネットワーク ユーザに適切なアクセス レベルを割り当てます。たとえば、ISE を使用して次のセキュリティ ポリシーを設定できます。

- 企業ネットワークを使用する任意の訪問者向けの**ゲスト アクセス** ポリシー
- iPad やスマートフォンなどの個人用デバイスを使用する従業員向けの **BYOD アクセス** ポリシー
- 企業ポリシーに適合していないと考えられるか侵害されているデバイスに対する、ネットワークへの**ゼロ アクセス**
- IT 部門によって割り当てられたデバイスを使用している従業員向けの**ビジネスクラス アクセス**
- 企業ワークステーションを使用する経営幹部向けの、機密情報への**高度なアクセス**

ネットワークから収集したすべてのコンテキスト データを利用して、Cisco ISE は、いつどんなときでも適切なレベルのアクセスを適切なユーザに提供し、非準拠または侵害されているデバイスがそもそもネットワークにアクセスしないようにして、潜在的な攻撃対象領域を制限します。

これと同じコンテキスト データを Lancope StealthWatch と共有することで、アラートをトリガーした IP アドレスについての詳細情報を提供できます。この統合を通じて、Lancope は IP アドレスに関する追加情報を ISE に要求できます。Lancope のダッシュボードで、潜在的なネットワークの脅威または悪意のあるアクティビティのトリアージと分析に必要な、詳細な可視性を自動的に取得することが可能になりました。この追加データによって、ネットワークから提供される NetFlow データから短時間で情報を引き出すことができます。

ルールを設定しエンフォーサとしてネットワークを活用する

ネットワーク全体がセキュリティ センサーに転換されると、組織はネットワークに接続しているのが誰または何で、ネットワークで何をしているか、詳細に把握することができます。悪意のある攻撃が発生した場合、組織にとってよくない状況が目に入ります。幸いにも、シスコのお客様はこうした場合でもセキュリティの脅威に対処して解決するためのテクノロジーをすでに所有しています。ただ機能を有効にするだけで解決できるのです。

Cisco ISE が組織を保護する方法の 1 つは、Cisco TrustSec ソフトウェア定義型セグメンテーション テクノロジーの活用です。TrustSec ソフトウェア定義型セグメンテーションをみなさんに理解してもらうため、このセクションでは特長と ISE との関係を説明します。

Cisco TrustSec ソフトウェア定義型セグメンテーションは既存のシスコ インフラストラクチャに埋め込まれたテクノロジーで、ソフトウェア定義型セグメンテーションを使用してマルウェア伝播のリスクを軽減し、ネットワーク全体への拡散を防止し、脅威を封じ込めます。トラフィックの分類は、IP アドレスではなく、ユーザ/デバイスの役割に基づいて実行されます。Cisco ISE を使用して TrustSec ソフトウェア定義型セグメンテーションを利用するポリシーを作成すると、ネットワーク アクセスのプロビジョニングと管理を簡素化し、セキュリティ運用を効率化し、ネットワークのどこででもセグメンテーション ポリシーを一貫して適用できます。前述のように、Cisco ISE はネットワークにアクセスしているのが誰で何かについて、高度なコンテキスト データを収集します。その後で、ネットワークをセグメント化するセキュリティ グループ タグを使用して、ロール ベースのアクセスを定義します。この一元化されたソフトウェア定義型セグメンテーション ポリシーは、ネットワーク全体でポリシー決定を適用するために、ISE によって TrustSec ソフトウェア定義型セグメンテーション対応ネットワーク デバイスにプッシュされます。

ソリューションを連携させる

Cisco IOS Flexible NetFlow、Cisco ISE、Lancope StealthWatch および Cisco TrustSec ソフトウェア定義型セグメンテーションを組み合わせることで、最終的にはお客様の既存のインフラストラクチャ投資を最大化してネットワークのセキュリティを改善できます。

たとえば、デバイスがネットワークに接続されると、トラフィックは NetFlow と Lancope StealthWatch の統合によって常に監視および分析されます。異常なアクティビティが検出されると、管理者は ISE の統合によって、イベントをユーザ、デバイス、場所にすばやく関連付けることができます。

不審な活動があると判断された場合は、攻撃しているデバイスまたはユーザを TrustSec ソフトウェア定義型セグメンテーションと ISE によるネットワーク分離に迅速に配置できます。その結果、隔離されたデバイスはネットワークに分離され、IT 部門はそれを特定して緩和できます。感染の有効な「爆発半径」は縮小され、さらなる被害が回避されます。

これらのソリューションが連携すると、ネットワーク管理者は、センサーおよびエンフォーサとしてのネットワークの役割によって、環境に対する可視性とコントロールを獲得できます。

セクション IV：まとめ

デジタル エコノミー、変化するビジネス モデル、そして動的な脅威状況が取り巻く中、侵害から復旧までの時間を短縮するための組織のアプローチを統合し、普遍的かつ連続的でオープンなものにする必要があります。

IT 部門の課題は、従来のエンドポイントおよび境界を重視したセキュリティでは不十分だということです。これらのセキュリティ テクノロジーは、ほぼセキュリティ侵害の発生防止のみを目的としています。もちろんこれも非常に重要ではありますが、セキュリティ インシデントが発生した時点で検出して、水平に感染したりデータが流出したりする前に修復することに、より注力される必要があります。

ネットワークをセンサーおよびエンフォーサとして使用することで、ビジネスを保護し、セキュリティ環境に対する他にないレベルの可視性を実現できます。シスコのセキュリティおよびネットワーク ポートフォリオは多岐にわたり、シスコは、これらの分野で市場リーダーであることから、ネットワークをセンサーおよびエンフォーサに転換するビジョンを実現するという、独自の地位を獲得しています。

シスコのお客様のほとんどは、今お持ちのテクノロジーを使用して、今すぐこの移行を開始できます。機能はシスコのネットワーク ポートフォリオまたはルータやスイッチに組み込みのコンポーネントだからです。

詳細な可視性とコンテキスト情報へのアクセスによって得られる実用的な知見を自動化して、現在のサイバー犯罪者と戦う企業を支援します。セキュリティのためにネットワークを活用することをぜひご検討ください。