分断されたセキュリティサイロの課題

イベント情報の相関分析による、インシデントレスポンス

10 箇所に拠点を持つ大規模な組織でも、従業員 10 人程度の中小企業であっても、導入している複数のセキュリティ製品やソリューションが相互に連携することが出来なければ、セキュリティ対策における高い効果を得ることは難しくなります。 IT チームが本社と各拠点の情報を包括的に扱ったり、整合性のないネットワークやエンドポイントソリューションを運用する場合には、このようなセキュリティサイロが大きな問題となります。

サイロ型のセキュリティ運用になっていませんか?

1

すべての規模の組織においてセキュリティの脅威が拡大している中、複数のセキュリティ製品が後付けで、追加導入されています。特定のセキュリティの課題を解決するための新たな製品が既存の環境に追加されてきました。このような環境では、セキュリティソリューションが相互に連携することがなく、セキュリティ体制がサイロ化されてしまいます。

2

複数の分散拠点をもつ企業では、適用されるセキュリティ機能が各拠点と本社間で一貫していない場合があります。各拠点毎にセキュリティレベルが異なることは、理にかなっていますが、一方では、IT チームが複数のセキュリティシステムや拠点の管理作業が必要な個々のサイロが発生します。

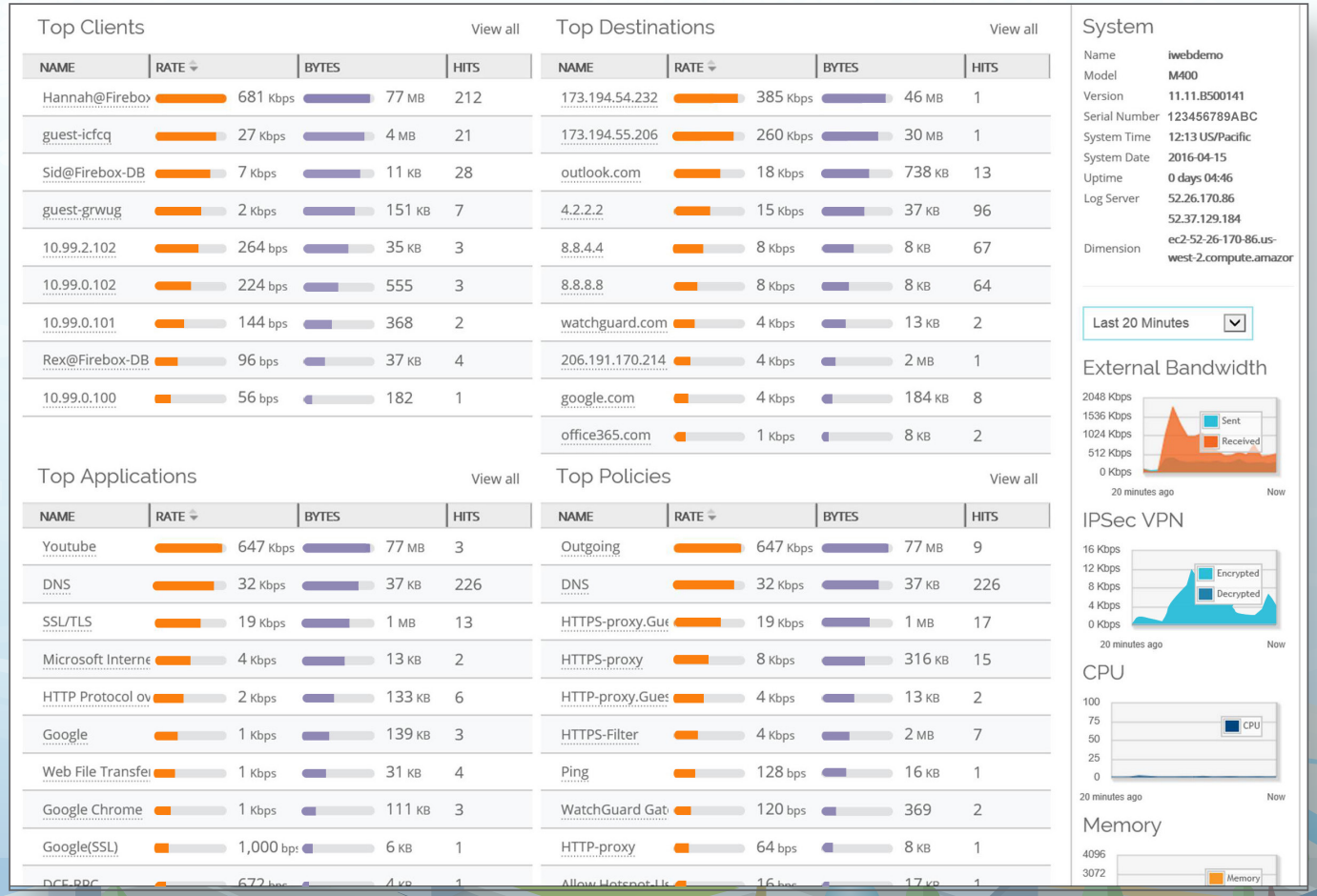
3

リモートで業務を行う従業員は、ファイアウォールによる保護を受けることができずに、脅威の影響を受けやすくなります。これらのリモートデバイスを完全に把握していないと、ネットワークへの侵入を試みるハッカーに簡単に攻撃経路として悪用される恐れがあります。

セキュリティ対策はネットワークから

ネットワークトラフィックは、セキュリティに関する最も重要な情報源です。異常またはブロックされたトラフィックパターン、悪意のある Web サイトや危険な Web サイトへのアクセスを可視化し、ボットネットやその他の脅威を検出できるようにすることは、組織を保護するための最も重要なステップの 1 つです。ネットワークに接続されているデバイスを把握することも重要です。適切な権限があり、適切なセキュリティポリシーが適用されている場合にのみアクセスできるようにすることが重要です。

ネットワーク上で発生している状況を把握することで、使用状況を基準にスループットとパフォーマンスへの影響に関する情報を利用できるようになります。多くの帯域幅を利用しているユーザーとその利用目的を可視化する事は、パフォーマンスの低下を防ぐためにも、非常に重要です。



ネットワーク

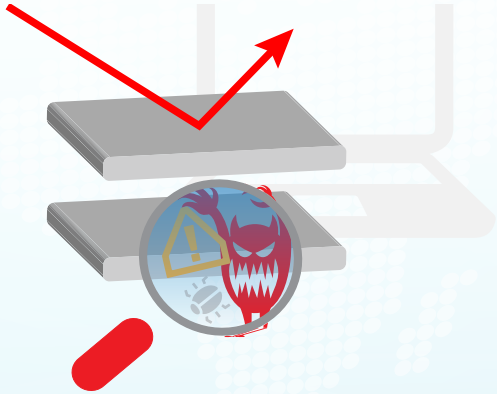
エンドポイント

エンドポイントソリューションの検討

エンドポイントの可視化は、デバイスを把握し、デバイスを保護するための適切なセキュリティが適用されていることを確認することから始まります。特に、脅威の影響を受けやすいユーザーや、すでに感染済みのユーザが存在していないかを知ることも重要です。

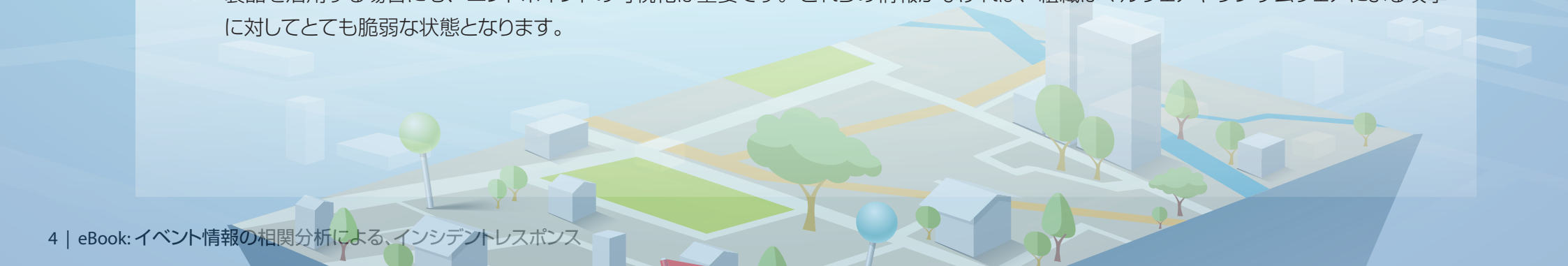
実際に、エンドポイントを保護するための可視化には以下の **2つのレイヤー**が重要です

把握している脅威をブロック / 把握できていない脅威の特定



シグネチャのアップデートに依存する既存のアンチウイルスソリューションは、既知の脅威を阻止する場合には最適です。
しかし、パッチやシグネチャの更新は毎週または必要な時にのみ実行されるため、この保護レイヤーには弱点があります。

未知のゼロデイの脅威を検知することは、簡単ではありません。ある事象が脅威であるかどうかを判断する方法は、セキュリティソリューションによってさまざまです。ヒューリスティックエンジン、挙動分析、ファイル、プロセス、レジストリの変更をトラッキングするような製品を活用する場合にも、エンドポイントの可視化は重要です。これらの情報がなければ、組織はマルウェアやランサムウェアによる攻撃に対してとても脆弱な状態となります。



脅威インテリジェンスの活用でスマートな対策

ガートナーは、脅威インテリジェンスを「資産に対する既知または新たな脅威に関する、コンテキスト、メカニズム、指標、予測、実効的なアドバイスを含む証拠ベースのナレッジであり、脅威に対応するための意思決定に使用できる情報」と定義しています。

簡潔に言えば、脅威インテリジェンスとは、既知または公開済みの脅威について把握しているすべての情報の集合であり、脅威を阻止できるようにユーザに通知すべき重要な分析情報です。この情報の分析作業は多くの時間とリソースが必要となります。現在、このようなソリューションの開発に積極的に取り組んでいるベンダは、多数存在しており、高額なソリューションとして、主に大企業にサービスを提供しています。

無償で提供されている脅威情報も多くありますが、有料の情報は非常に有用であることを理解しておく必要があります。無料の脅威情報は通常、定期的に更新されないため、直近で検知された最新の脅威が含まれていない可能性があります。エンタープライズグレードの脅威インテリジェンスフィードを連携させる事で、最高の効果を発揮する事が可能ですが、中堅中小企業にとっては高価な情報を活用するためのコストが課題になる場合があります。

しかしながら、中堅中小企業が直面している脅威は日々増大しており、これらの脅威に対抗するために、脅威インテリジェンスの重要性は日々増加しています。ほぼリアルタイムで更新され、組織に深刻な被害を及ぼす恐れがある既知の脅威について最も正確なデータを提供する、中堅中小企業でも活用可能な脅威インテリジェンスが必要となっています。

相関分析によるすべての情報の統合

ネットワーク、エンドポイント、および脅威インテリジェンスフィードから個別に収集される豊富な情報は、組織を保護する上で非常に重要です。しかし、このデータが分断されたセキュリティソリューションで利用されている場合には、発生している脅威情報を的確に把握することは困難です。これらの情報をすべて相関分析することで最高の効果を得ることができます。

相関分析によって、さまざまな情報ソースが新しい次元で可視化されるようになります。イベントデータを一元的に収集して組み合わせることで、組織は実用的なインサイトを獲得し、実効性の高い対策が可能となります。IT チームはこの情報を解析して優先順位を付けることで、自社のビジネスを脅かすセキュリティの脅威に対して、自信を持って対応することができます。攻撃の検知までの時間を短縮し、最も重大な攻撃に対して、効率的かつ効果的な対応を講ずることが可能になるため、時間とリソースが限られている組織にとって大きなメリットがあります。

相関分析

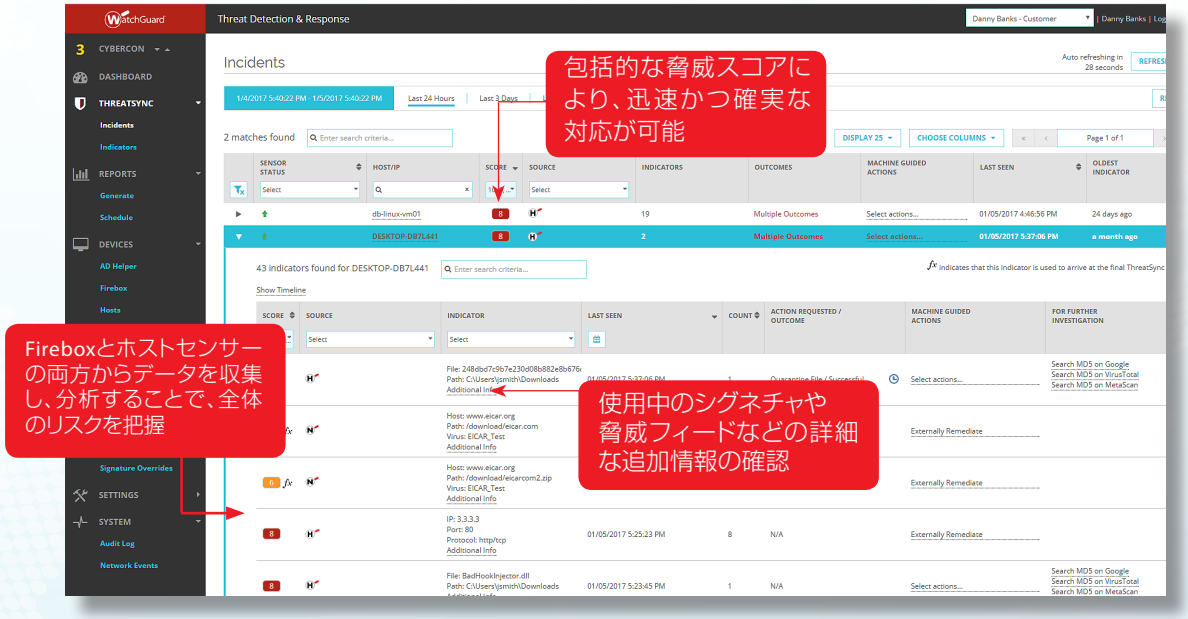
相関分析、重要度による優先順位付け、レスポンス

相関分析がそれほど重要であるのならば、なぜこれまで採用されてこなかったのでしょうか？

現在まで、相関分析は非常に複雑で、特に自動化が困難だったためです。

ウォッチガードは、エンタープライズクラスの相関分析機能を持つ最新のセキュリティサービスである Threat Detection and Response (TDR) を中堅・中小企業および複数拠点を持つ企業に提供します。

ThreatSync は、TDR のクラウドベースのスコアリングおよび相関分析エンジンのコンポーネントであり、Firebox® およびエンドポイントにインストールされる WatchGuard Host Sensor、サードパーティの脅威インテリジェンスフィードの脅威データをもとに相関分析を実行します。ThreatSync はさらに、脅威の重要度に基づく包括的な脅威スコアを作成し、これにより被害が発生する前に、脅威に対応するための実効的なインテリジェンスを管理者に提供します。



Threat Detection and Response (TDR) は Total Security Suite ライセンスに含まれており、ライセンスに含まれている APT Blocker, WebBlocker, RED（Reputation Enabled Defense）などのセキュリティ機能からの情報も収集して活用します。

ウォッチガードは、これらの先進的なセキュリティサービスをすべて 1 つのソリューションとして提供する唯一のセキュリティアプライアンスベンダであり、あらゆる企業に強力な相関分析のメリットを提供できる唯一のベンダです。

ウォッチガードの Threat Detection and Response サービスは、ネットワークとエンドポイントのセキュリティ対策を統合し、エンドポイントまで可視化を拡張することで、早期にセキュリティの脅威を検知し、修復までの時間短縮と企業のインシデントレスポンスを支援する業界最高クラスのソリューションです。

WatchGuard® Technologies, Inc. は、業界標準のハードウェア、ベストインクラスのセキュリティ機能、およびポリシーベースの管理ツールをインテリジェントに組み合わせた、統合型セキュリティソリューションを提供するグローバルリーダーです。ウォッチガードは、管理性の高い優れたセキュリティソリューションを世界各国の数千以上の企業に提供しています。

詳細は、WatchGuard.co.jp/TDR をご覧ください。