WatchGuard Threat Detection & Response (TDR)

狙われる中堅中小企業のセキュリティ

ニュースの見出しには、大企業へのサイバー攻撃の報告があふれています。しかしながら、メディアから報道されるニュースでは、中堅中小企業が同様のサイバー攻撃の被害を受けているとは報じていません。実際に米国証券取引委員会（SEC）は、中堅中小企業がサイバー犯罪の主な標的になっていると報告しています。 2014年には、すべてのサイバー攻撃の対象の60% が中堅中小企業となっており、スピアフィッシングによる攻撃の標的の75% が中小企業との報告があります。

2014年、サイバー攻撃の対象の**60%**が**中堅中小企業**

スピアフィッシングによる攻撃の標的の**75%**が**中堅中小企業**

これらの企業にとって、これらの攻撃への対策をより困難にするのは、やはり関連するコストです。被害を受けた企業の約半数がサイバー攻撃から6ヶ月以内に事業を終了しています。中堅中小企業であっても大企業と同様にサイバー攻撃の標的になりますが、セキュリティ対策に割り当てられる予算は比較的小さく、十分な人員リソースがない場合があります。では、中堅中小企業は、限られたリソースの中で、効果的にサイバー攻撃に立ち向かうにはどうしたらよいのでしょうか？

シグネチャベースのセキュリティ対策の限界

攻撃者は、セキュリティベンダーの開発技術を把握しているかのように、ウイルス対策ソフトウェアをすり抜ける新種のマルウェアを作成しています。マルウェアが検知される前に、いくつかの企業は、感染される事が予想されますが、セキュリティベンダーはすぐに新種のマルウェアを阻止するためのシグネチャを作成します。それらが数回ブロックされると、攻撃者はマルウェアを完全に放棄するか、シグネチャでの検知を回避するために難読化などの変更を行い、変異型のマルウェアを作成します。このように、新たなマルウェアの異種の発生とシグネチャのアップデートの一連のプロセスが繰り返されているのが実情です。

近年、シグネチャベースの対策ではなく、別の方法でマルウェアを検知する方向に向かっています。セキュリティベンダーは、マルウェアの振舞いや行動パターンによりマルウェアを特定してブロックすることで、マルウェアの機能を防止し、封じ込めようと考えています。すべてのマルウェアの異種が同じように動作するわけではありませんが、マルウェアの検知率を改善するためにトラッキングできる共通の動作がいくつかあります。

マルウェアを振舞いベースで把握

現時点で、多くのマルウェアは、さほど特異な振る舞いや行動パターンは行っていません。ハッカーは常に進化し、攻撃方法を変えていますが、ほとんどのマルウェアには一貫した行動パターンの傾向が確認出来ます。

マルウェアの振舞いの特長

- マルウェアをダウンロードして実行させるために、Microsoftのマクロに潜入する
- 検知を遅らせるために、感染後に自身を削除して痕跡を残さないようにする
- OSのカーネルレベルでのアクセス制御を回避するために、管理者権限を取得しようとする
- 悪意のあるコンポーネントを挿入し、ファイルやプロセスを変更する
- オリジナルのシステムファイルを削除し、同じファイルタイプと名前の偽装ファイルに置き換える

既知の脅威に対しては、シグネチャによる検知は重要な防御となりますが、未知のマルウェアや新種のマルウェアやその亜種に関して、阻止する手段が必要です。
上記のような行動の組み合わせを追跡することで、シグネチャで検知できないマルウェアの亜種を検知することができます。

TDR による検知

ウォッチガードの最新セキュリティサービスであるThreat Detection and Response（ＴＤＲ） は、WatchGuard Host Sensor に実装されている複数の検知技術を使用して、高度なマルウェアの脅威を検知します。

シグネチャ - マルウェアとの闘いにおいて重要な防御線です。様々な情報源から収集された既知の脅威に関する最新の情報を持つ必要があります。TDRは、最新の脅威情報フィードをから、エンドポイントの疑わしいイベントが既知の脅威であるかどうかをリアルタイムに確認します。

振舞いによる検知技術 - シグネチャベースでの検知技術だけに頼るのではなく、TDRはルールセットまたはアルゴリズムを使用して、悪質な行動となる可能性のあるコマンドを検知します。この検知技術は、悪意あるコマンドが実行される前に、迅速に脅威となる活動をマークします。TDRは WatchGuard Host Sensor を通じて175以上の振舞いパターンを活用して監視します。

行動分析 - マルウェアの脅威は特定の動作パターンに従う傾向があるため、それらのステップを追跡することで、見えないマルウェアの亜種を確実に検知できます。Host Ransomware Prevention（ＨＲＰ）機能は、ランサムウェア攻撃に関連する動作を追跡し、ファイル暗号化が行われる前にこれらの攻撃を防止します。

ネットワークの検知 - ネットワークは、マルウェア攻撃およびネットワーク利用でのパフォーマンスに関する重要な情報源です。異常なトラフィックパターンやブロックされたトラフィック、悪意のあるWebサイトやリスクの高い危険なWebサイトへの訪問、ボットネットやその他の脅威を監視しる事は、組織を保護するうえで不可欠です。 TDRはWatchGuard の最先端の高度なネットワークセキュリティ機能を活用して、ネットワーク上の脅威情報を収集して検知します。

相関分析の効果

さまざまな情報源からデータを収集する事は重要ですが、収集だけでは意味を持ちません。それらの情報源が完全に別々に扱われている場合には、情報源からの包括的な知見は提供されません。相関分析は、これらのセキュリティソリューションから生成される情報を収集し、重要なポイントを関連付けして理解します。複数のセキュリティ機能からのセキュリティ情報を関連付けして分析することにより、脅威の検知と修復に必要な時間を短縮し、IT管理者がどの脅威が最も深刻であり、直ちに注意が必要かを明確に把握する事ができます。

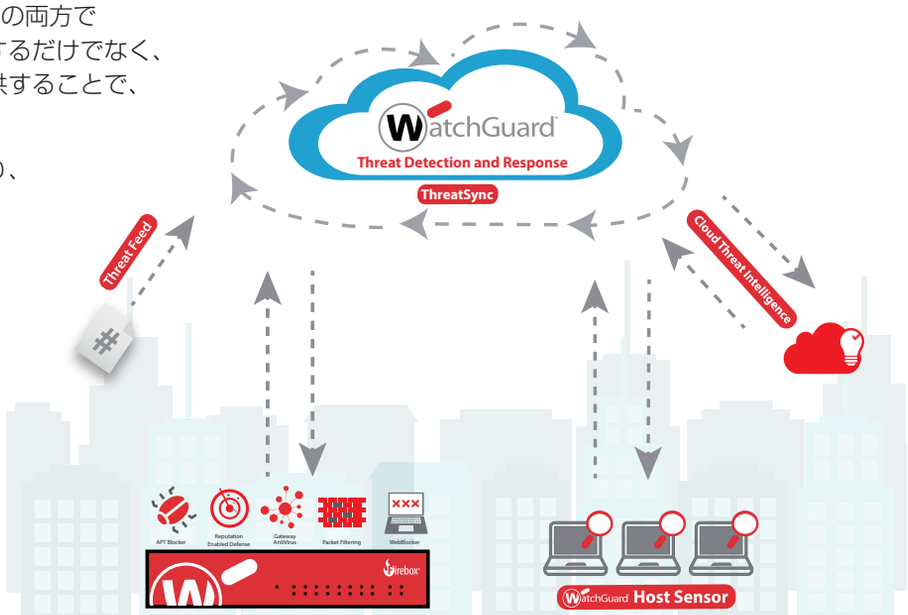
ThreatSync で脅威をスコアリング

相関分析エンジンを通じてセキュリティイベントを確認することは、組織のセキュリティ状況を完全に把握する唯一の方法です。 WatchGuard のクラウドベースの相関分析および脅威スコアリングエンジンであるThreatSync は、ネットワークとエンドポイントの両方を攻撃する脅威に対する実用的な洞察を提供します。

独自のアルゴリズムにより、ThreatSync はセキュリティイベントに包括的な脅威スコアリングを行い、レスポンスが必要と考えられるインシデントに対して、優先順位付けを行います。

ThreatSync は、ネットワークとエンドポイントの両方で
発生しているセキュリティイベントを可視化するだけでなく、
包括的な脅威のスコアリングと優先付けを提供することで、
注意すべき重要度の高い脅威を検知します。

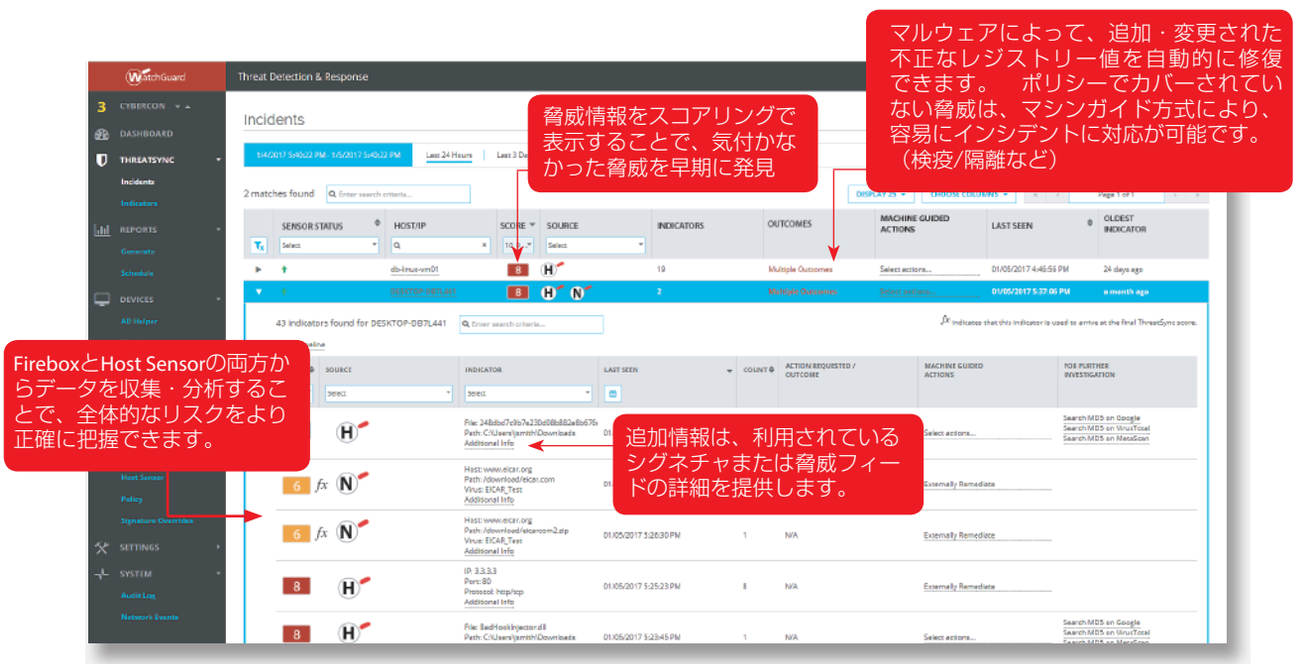
また、脅威の重要度による優先順位付けにより、
組織は検知と修復までの時間を短縮し、
修復するために必要な企業内のリソースを
節約することが可能です。



TDRによるインシデントレスポンスの自動化

セキュリティ管理者のリソースが不十分な中堅中小企業や専任のIT管理者のいない分散拠点などでは、セキュリティの脅威に関する監視や管理が困難な場合があります。インシデントレスポンスの自動化は、脅威の迅速かつ効果的な検知と修復のための重要な鍵となります。脅威へのレスポンスを自動化することで、組織は担当者やセキュリティ管理者の負荷を軽減し、他の重要なセキュリティ分野に注力することが可能となります。また、自動的なレスポンスにより、企業のマルウェアからの修復と組織が正常な運営に復旧するための時間を大幅に短縮します。

TDRを使用すると、組織のニーズに基づき、対応の自動化を可能にするポリシーを容易に設定できます。 ThreatSync によって提供される脅威スコアリングと優先順位付けにより、ユーザーは、プロセスの停止、ファイルの隔離、変更されたレジストリ値の正常化など、脅威のスコアまたは適用範囲に基づいて修復するポリシーを設定し、開始できます。たとえば、攻撃を受けるリスクが低い組織で、8以上のスコアをつけた上位の脅威に対する自動での対応を設定したり、攻撃のリスクが高い場合には、6以上のスコアで自動的に脅威を修復することを選択できます。



Host Ransomware Prevension(HRP)に関する詳しい情報は,
www.watchguard.co.jp/TDR

ウォッチガードについて

WatchGuard® Technologies, Inc. は、ネットワークセキュリティ、セキュア Wi-Fi、ネットワークインテリジェンス製品、セキュリティサービスの世界的なリーダーであり、世界各国の75,000社以上のお客様にサービスを提供しています。ウォッチガードのミッションは中堅中小企業や多拠点をもつ分散型企業向けの理想的なセキュリティソリューションを提供し、すべての企業がエンタープライズグレードのセキュリティを容易に利用できるようにすることです。ウォッチガードの本社は、米国ワシントン州のシアトルにあり、北米、欧州、日本、アジア太平洋地域、および南米にオフィスを展開しています。
詳しくはWatchGuard.co.jp をご覧ください。

ウォッチガード・テクノロジージャパン株式会社　〒106-0041 東京都港区麻布台1-11-9 BPRプレイス神谷町5階　Tel:03.5797.7205　Fax:03.5797.7207
Mail: JPNSALES@watchguard.com