Threat Detection & Response

相関分析、重要度による優先付け、レスポンス

サイバー犯罪者は、企業ネットワークにアクセスするために、あらゆるコネクションポイントから様々な手法を複合的に駆使して、複雑かつ高度な攻撃を行います。効果的なセキュリティ対策には、ネットワークとエンドポイント両面からのセキュリティ検知機能が必要なだけでなく、攻撃者の目的からなる活動内容も含めた分析が必要です。ウォッチガードの Threat Detection and Response（TDR）は、ネットワークとエンドポイントのセキュリティイベント情報を脅威インテリジェンスを活用した相関分析を行い、攻撃の検知とイベントの重要度に基づく優先順位付けを行い、マルウェア等による攻撃を速やかに阻止します。
企業のセキュリティ管理者やマネージドセキュリティサービスプロバイダ（MSSP）は TDR を活用して、重大な情報漏えいを未然に防止し、企業活動の生産性を低下させることなく、効果的にセキュリティ対策を強化します。

ネットワークとエンドポイントイベントの相関分析

ThreatSync はウォッチガードの新しいクラウドベースの相関分析エンジンと脅威スコアリングエンジンであり、セキュリティの脅威を鋭敏に検知し、ネットワークとエンドポイント全体におけるレスポンス能力を向上します。ThreatSyncは、WatchGuard Firebox 、WatchGuard Host Sensor からイベント情報を収集し、クラウド上の脅威インテリジェンスを活用した相関分析を行い、脅威スコアの生成と適切なセキュリティ脅威への対応を可能にします。

可視化機能をエンドポイントまで拡張

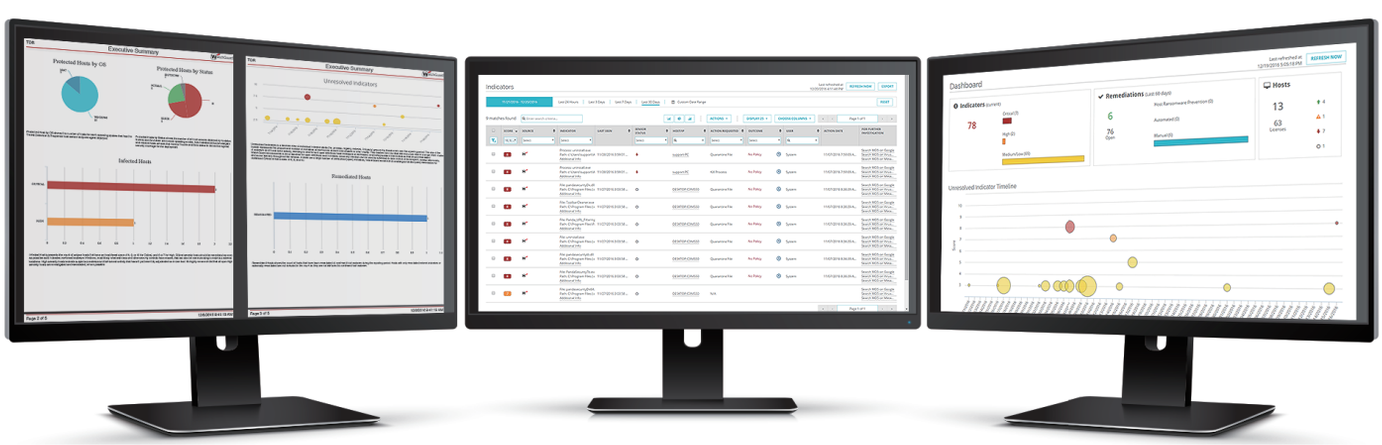
WatchGuard Host Sensor は、デバイスに負荷をかけることなく、脅威の監視および検知を可能にします。Host Sensor は、脅威イベント情報を継続的に ThreatSync に送信し、相関分析およびスコアリングを実行し、セキュリティの問題を修正する手順を生成し 、実行します。 Host Sensor はクラウド上で一元管理されるため、MSSP や IT管理者はあらゆる場所から容易に更新したり、管理する事が可能です。

エンタープライズグレードの脅威インテリジェンス

サードパーティベンダから収集される脅威情報は、これまで多くの予算と専任のセキュリティチームを擁する主に大規模な組織や企業が利用可能なソリューションでした。企業は TDR により 、管理を複雑にしたりコストを追加したりすることなく、容易に脅威インテリジェンスを活用し、企業内のセキュリティ状況の分析とレスポンスを実施できるようになります。

先進のランサムウェア対策

Host Ransomware Prevention(HRP）は、 WatchGuard Host Sensor に実装されているランサムウェアに特化したモジュールです。HRP は、挙動分析エンジンとデコイディレクトリ（ハニーポット)によって、特定の動作や処理がランサムウェア攻撃に関連しているかどうかを判別するために、エンドポイントでのさまざまな特性を監視します。悪意ある脅威と判定した場合に、HRP はエンドポイントでファイルが暗号化される前に自動的にランサムウェア攻撃を防止します。



〒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
https://www.watchguard.co.jp　JPNSALES@watchguard.com

ウォッチガード・テクノロジージャパン株式会社

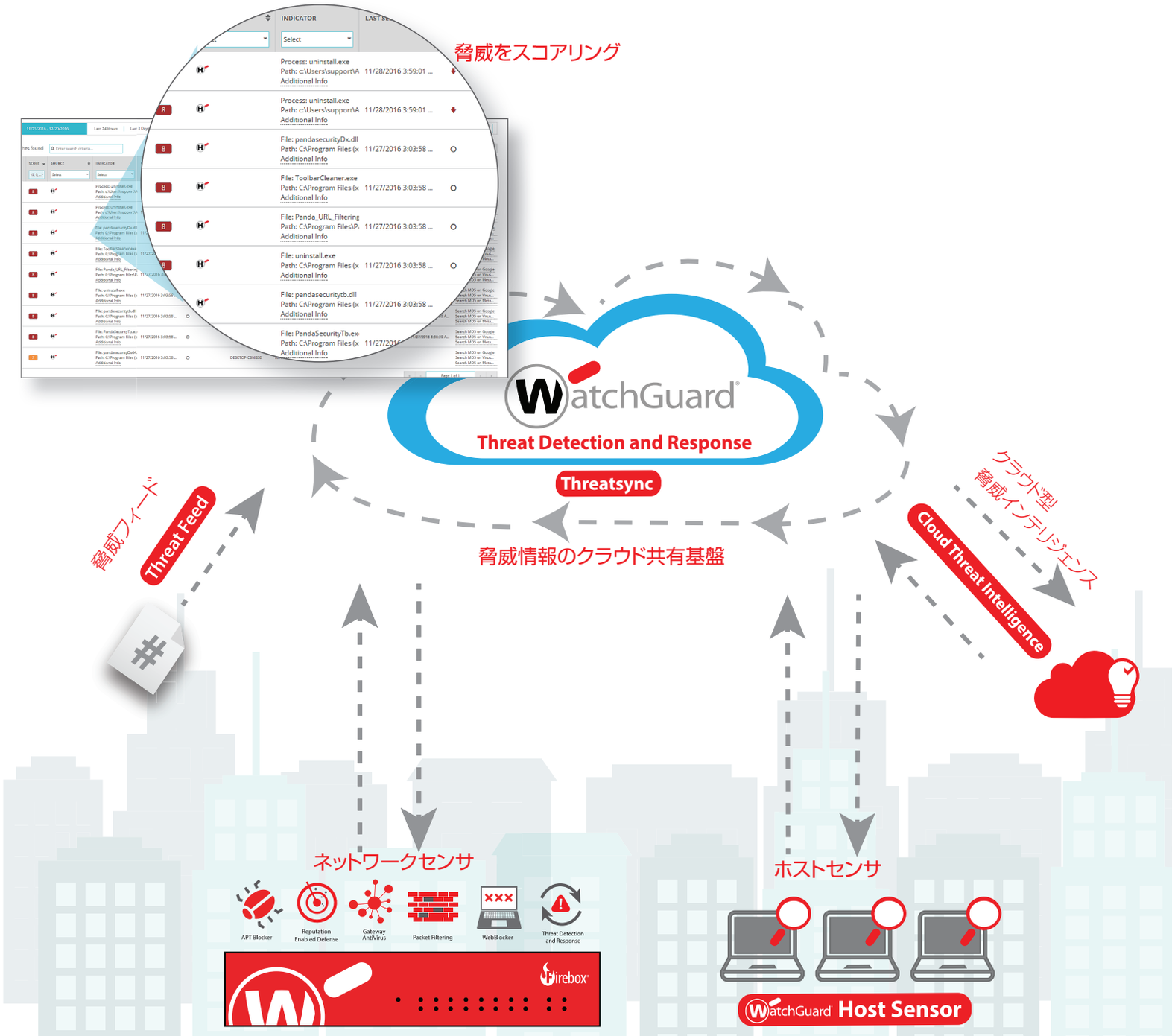
相関分析によるインシデントレスポンス強化

TDR のクラウドベースの相関分析および脅威評価エンジンである ThreatSync は、ネットワークとエンドポイント全体でセキュリティの脅威を鋭敏に検知し、対応能力を向上します。

ThreatSync は、APT Blocker、RED（Reputation Enabled Defense）、Gateway AntiVirus、WebBlocker などのFirebox上で動作する複数のセキュリティサービスからネットワークイベント情報を収集します。これらのイベント情報は、WatchGuard Host Sensor によって検出されたイベント情報とエンタープライズグレードの脅威インテリジェンスとで相関分析されます。

ThreatSync はこの脅威データから包括的な脅威スコアを生成し、重要度のをランク付けをします。その結果、ファイルの隔離、プロセスの強制終了、レジストリ値の削除などの脅威に対する特定の対応が Host Sensor に指示され、ポリシー設定による自動化を図ることが可能になります。

このウォッチガード独自のテクノロジーにより、ネットワークとエンドポイントの両方で脅威の可視化を強化し、脅威の検出するまでの時間の短縮と、包括的な脅威スコアによる迅速なレスポンスの自動化が可能となります。



One アプライアンス、One パッケージ、Total Security

TDRを利用するためのライセンスは、WatchGuard Total Security Suite に含まれています。WatchGuard Total Security Suiteには、APT Blocker、WebBlocker、Gateway AntiVirus、IPS、RED(Reputation Enabled Defense) などの高度なセキュリティソリューションも含まれています。

それぞれのセキュリティソリューションにより、対応する高度な脅威から組織を保護しますが、これらのセキュリティ機能を連携させる事で、Firebox のパフォーマンスに影響を与えることなく、高い効率性と堅牢なセキュリティ対策を実現します。

製品	Support	TOTAL SECURITY	Basic Security
ステートフルファイアウォール	✓	✓	✓
モバイルVPN	✓	✓	✓
ブランチオフィスVPN	✓	✓	✓
アプリケーションプロキシ	✓	✓	✓
不正侵入検知·防御 (IPS)		✓	✓
アプリケーションコントロール		✓	✓
URLフィルタリング (WebBlocker)		✓	✓
スパム対策 (spamBlocker)		✓	✓
ウイルス対策 (Gateway AntiVirus)		✓	✓
レピュテーションセキュリティ (RED)		✓	✓
Network Discovery		✓	✓
標的型攻撃対策 (APT Blocker)		✓	
情報漏えい防止 (DLP)		✓	
Dimension Command		✓	
Threat Detection & Response (TDR)		✓	
サポート	スタンダード (24x7)	ゴールド (24x7)	スタンダード (24x7)

Firebox モデル	同梱されるHost Sensors数
T10	5
T30	20
T50	35
T70 / M200	60
M300	150
M400 / M440 / M500 / M4600 / M5600	250
XTMv S	20
XTMv M	50
XTMv L	150
XTMv DC	250

Host Sensor を追加する場合

Threat Detection and Response の Host Sensor 数は、Firebox M シリーズ、T シリーズ、XTMv アプライアンスのそれぞれに Host Sensor 数の初期値が規定されています。組織内のデバイス数に応じてアドオンオプションを購入し、Host Sensor を追加する事が可能です。

Host Sensor アドオンオプション
10 Host Sensors
25 Host Sensors
50 Host Sensors
100 Host Sensors
250 Host Sensors
500 Host Sensors

優れた管理性とスケーラブルなインシデントレスポンス

Threat Detection and Response（TDR)により、企業規模の拡大に合わせて適用範囲をスケールアップし、容易にセキュリティ管理を実現する事が可能です。TDR は、クラウドベースのサービスであり、管理者は組織内のエンドポイントに Host Sensor をインストールすることで、ポリシーによる操作で容易にセキュリティの問題を修正できるようになります。

TDR は、ビジネスの成長に合わせて容易に拡張できます。TDR のライセンスは、Fireboxの機種毎に包含されている Host Sensor ライセンスで利用可能です。必要に応じて、Host Sensor を追加し、組織のニーズに合わせてインシデントレスポンス対策を拡張できます。

企業内のリソースでセキュリティの管理が困難な場合には、MSSPパートナを活用してセキュリティ関連業務をアウトソースし、TDRのさまざまなメリットを享受する事も可能です。

Threat Detection and Response の詳細をご覧ください。
最新のセキュリティサービスの詳細については、Webサイト（www.watchguard.co.jp/TDR）をご確認ください。

利用方法

ウォッチガードは、販売パートナーとセキュリティサービスプロバイダのネットワークを有しています。TDR をご利用の場合には、ウォッチガードの Web サイトから最適なパートナーをご確認ください。
購入方法など、ご不明な点があれば、ウォッチガード営業部までお気軽にご連絡下さい。

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企業であり、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。