DATASHEET

HOST SENSOR

Threat Detection and Response コンポーネント

エンドポイントの監視とインシデントレスポンス対応

セキュリティの脅威は日々進化し続けており、ネットワークからエンドポイントまでをあらゆる攻撃方法から保護する事が、ますます重要になっています。ウォッチガード Total Security Suite に含まれる Threat Detection and Response（TDR）サービスは、ネットワークとエンドポイントから発生するセキュリティイベント情報を脅威インテリジェンスと相関分析し、攻撃の検知、重要度の優先順位付けによって、マルウェアによる攻撃を迅速に阻止します。WatchGuard Firebox® アプライアンスからのネットワークイベント情報、エンドポイン上の WatchGuard Host Sensor からのイベント情報が自動的に収集されます。

WatchGuard Host Sensor は、エンドポイントにおける脅威を継続的に検知し、問題を修正するコマンドを受信し、実行が可能です。WatchGuard Host Sensor の機能の 1 つである Host Ransomware Prevention（HRP）は、高度なマルウェア防御機能を提供する APT Blocker と共に利用する事で、ランサムウェアに対して業界最高レベルの保護を実現します。HRP は、エンドポイントでファイルが暗号化される前に、ランサムウェアの実行をブロックし、被害が発生する前にランサムウェアの攻撃を防御します。

ネットワークの可視化をエンドポイントまで拡張

軽量な WatchGuard Host Sensor は、デバイスに負荷をかけることなく、ヒューリスティックエンジンおよび挙動分析エンジンにより、セキュリティの脅威を監視、検知します。Host Sensor は、これらのイベントを TDR の ThreatSync に継続的に送信し、Firebox アプライアンスからのイベント情報との相関分析により、包括的な脅威スコアを生成し、重要度による優先順位付けを行います。

脅威の自動的な修復

WatchGuard Host Sensor を使用すると、作成したポリシーに基づいて脅威による変更の修復を自動化する事が可能です。これらの定義済みのポリシーは、ThreatSync によって生成された包括的な脅威スコアに基づいて、プロセスの強制終了、ファイルの隔離、レジストリ値の削除などの対応を決定します。

脅威の修正を自動化することにより、インシデントレスポンス対応時間を短縮でき、限りあるリソースへの需要を最小限に抑えることもできます。

高度な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対策のためのモジュールです。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）を利用して、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役立つさまざまな特性を監視します。悪意のある脅威である場合、HRP は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ブロックします。

機能と利点

- エンドポイントの脅威イベントを継続的に監視して検知
- 自動化により、検知から修復までの時間を大幅に短縮
- ランサムウェアを含む高度なマルウェア攻撃に対しても有効な最新技術による防御を実現
- ポリシー設定により、プロセスの強制終了、ファイルの隔離、レジストリ値の削除などの自動実行が可能
- 軽量なソフトウェアエージェントとして、CPU リソースをほとんど消費しない
- 既存のアンチウイルスソフトウェアとの共存が可能

〒106-0041 東京都港区麻布台 1-11-9 BPR プレイス神谷町 5 階
Tel : 03.797.7205　Fax : 03.5797.7207　WEB www.watchguard.co.jp
ウォッチガード・テクノロジージャパン株式会社

DATASHEET

Host Sensor ライセンス

Total Security Suite のサブスクリプションをご購入されている場合、各アプライアンスで一定数の Host Sensor を利用できます。これらの Host Sensor は、Threat Detection and Response 内で管理および配布され、集約されたアカウントとして利用可能です。組織のニーズを満たすために、アドオン製品として Host Sensor を追加できます。

Firebox のモデル	Host Sensorsの数
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 アドオンオプション
10 個のHost Sensors
25 個のHost Sensors
50 個のHost Sensors
100 個のHost Sensors
250 個のHost Sensors
500 個のHost Sensors

HOST SENSOR の仕様

互換性のあるオペレーティングシステム

- Windows 7, 8, 8.1, 10
- Windows Server 2003, 2008, 2012
- Linux RedHat/CentOS 6, 7

Firebox T シリーズ , M シリーズ、および XTMv と互換性があります。

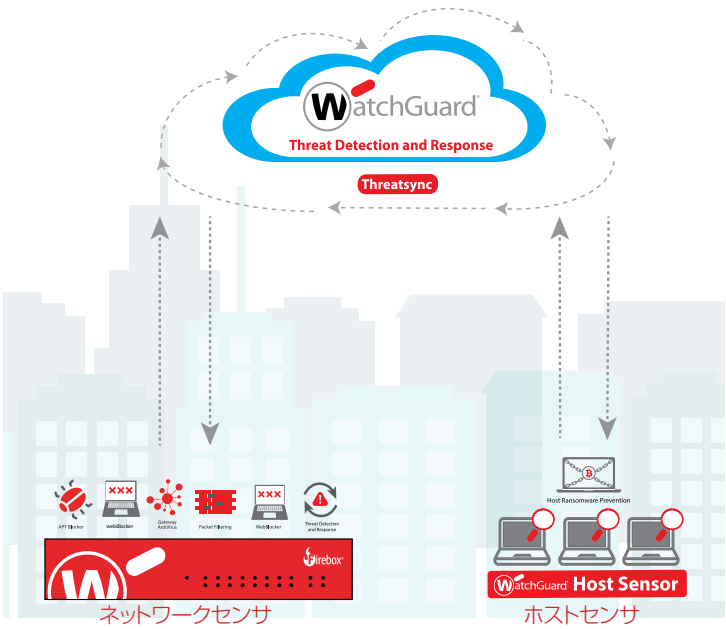
ウォッチガードのセキュリティサービス

1 台のアプライアンスと 1 つのパッケージで、包括的なセキュリティ対策を実現

複数のセキュリティ機能を連携させることで、ユーザは最高のセキュリティ保護と効率性、高速なネットワークパフォーマンスを実現し、最高の費用対効果を得ることができます。Total Security Suite は、基本となる Basic Security に加え APT Blocker, Data Loss Prevention(DLP), Threat Detection and Response（TDR）などの高度なセキュリティ機能を追加します。

TDR は、ネットワーク、エンドポイント、脅威インテリジェントフィードのイベントデータを相関させ、包括的な脅威スコアと重要度のよる優先付けをすることで、先進のセキュリティ環境を実現します。ThreatSync は脅威の相関分析とスコアリングエンジンであり、WebBlocker, APT Blocker, Gateway Antivirus, および spamBlocker などの高度なネットワークセキュリティサービスからも情報を収集します。その後、ネットワークイベント情報を、WatchGuard Host Sensor から収集したエンドポイントのイベント情報と相関分析し、重要度に基づく脅威スコアと優先順位付けを生成します。 組織は Total Security Suite を使用することで、高度なネットワークセキュリティ、エンドポイントの可視化と修復機能、エンタープライズグレードの脅威インテリジェンスを 1 つの包括的な製品として活用できます。

サービス	TOTAL SECURITY	Basic Security
侵入防止サービス (IPS)	✓	✓
アプリケーションコントロール	✓	✓
WebBlocker (URL/コンテンツフィルタリング)	✓	✓
spamBlocker (スパム対策)	✓	✓
Gateway AntiVirus (GAV)	✓	✓
Reputation Enabled Defense (RED)	✓	✓
Network Discovery	✓	✓
APT Blocker	✓	
Data Loss Prevention	✓	
Dimension Command	✓	
Threat Detection and Response (with WatchGuard Host Sensor)	✓	
サポート	ゴールド (24x7)	スタンダード (24x7)



ウォッチガードは、業界最大の付加価値リセラーとサービスプロバイダのネットワークを有しています。HP より、ウォッチガード認定パートナーをご確認いただけます。
Threat Detection and Response と WatchGuard Host Sensor の詳細については、watchguard.com/TDR をご覧ください。

www.watchguard.co.jp

Part No. WGJPTDR5_012017