ウォッチガード、次世代サンドボックスによるマルウェア検知・自動レスポンスを機能拡張

2017年9月27日（水）

ー企業向け統合型セキュリティプラットフォームのグローバルリーダであるWatchGuard（R）Technologiesの日本法人、ウォッチガード・テクノロジー・ジャパン株式会社（本社：東京都港区、社長執行役員
根岸正人、以下ウォッチガード）は、中堅・中小企業（SMB）、分散拠点を持つ大企業、およびマネージドセキュリティサービスプロバイダ（MSSP）を対象とした、クラウドベースのThreat Detection and
Response（TDR）サービスの機能アップデート版のリリースを発表しました。同サービスでは、脅威インテリジェンスを活用し、ネットワークおよびエンドポイントのセキュリティイベントを相関分析することで、マルウェアを検知し、優先順位付けを行い、迅速にレスポンスすることにより、サイバー攻撃を阻止することが可能になります。今回リリースしたTDRバージョン5.1では、エンドポイントのHost Sensorと次世代クラウドサンドボックスソリューションであるAPT Blockerがダイレクトに連携します。これにより、APT
Blockerの機能を、企業ネットワークへの接続状況にかかわらず、エンドポイントにも適用できるようになります。今後、IT管理者やMSSPは、クラウドサンドボックス上で不審なエンドポイントファイルを自動で分析することが可能となり、標的型攻撃、ゼロデイ攻撃、および回避型マルウェアの特徴的な振る舞いを特定し、迅速かつ確実にエンドポイントの脅威に対処することができます。

ウォッチガードのプロダクトマネジメント担当シニアバイスプレジデントであるアンドリュー・ヤング（Andrew
Young）は、次のように説明しています。「TDRは、包括的なUTM（統合脅威管理）ネットワークセキュリティサービスと、エンドポイントの検知・レスポンス機能を組合せた唯一のソリューションです。今回のTDRの最新アップデートでは、さらに能力を高め、APT
Blockerの高度なサンドボックス機能をネットワークからエンドポイントにまで拡張させています。今回のアップデートにより、潜在的に危険度の高いエンドポイント上でのファイルの振る舞いの特徴や目的をつぶさに観察して、マルウェアを防止するための適切な処理を自動で行うことが可能になります。」

TDRは以下のキーとなるいくつかの要素を組合せ、ネットワークとエンドポイントの両方で回避型の脅威を検知・レスポンスする能力を高めることができます：
・ ThreatSync –
ウォッチガードのクラウドベースの相関分析エンジンであり、Fireboxアプライアンス、Host Sensor、エンタープライズグレードのクラウドインテリジェンスフィードからリアルタイムでイベントデータを収集します。その後、これらのデータを分析することで総合的な脅威スコアを算出し、シングルクリック、もしくはポリシーに基づき、自動で脅威へのレスポンスを実現します。

・ UTMネットワークセキュリティ – ネットワーク上のWatchGuard Firebox M Series、T

Series、Firebox V、Firebox
Cloudアプライアンス、並びに既存のセキュリティサービスで生成されるセキュリティデータを収集し、ThreatSyncにより相関分析されます。

・ Host Sensor –
エンドポイントデバイスにインストールされる軽量のエージェントソフトウェアであり、ネットワーク境界を越え、個々のデバイスにまで監視機能を拡張させることができます。これらのセンサから、不審なエンドポイントセキュリティイベントがThreatSyncとAPT
Blockerに送信され、分析、スコアリング、そして適切な処理が実行されます。

・ APT Blocker –
次世代サンドボックスを活用し、エミュレーションを行うことで、ネットワークとエンドポイントの不審なファイルを安全な環境で実行し、振る舞いを分析します。APT
Blockerのレスポンスに基づき、ThreatSyncにおけるスコアリングがアップデートされ、脅威の排除が自動的に行われます。

・ Host Ransomware Prevention (HRP) モジュール – エンドポイントのHost
Sensor内に実装される軽量のソフトウェアモジュールであり、行動分析によりランサムウェアを特定し、ランサムウェアがファイルの暗号化を実行する前に自動で不審なプロセスを強制的に停止させます。HRPで常に新種の攻撃を防御できるように、新たな標的型攻撃等の振る舞いや特徴は常時アップデートされます。

これまで、TDRはネットワークゲートウェイでの脅威分析にAPT
Blockerを活用してきましたが、今回のTDRのアップデートにより、エンドポイントと脅威データ分析との直接連携が可能となり、APT
Blockerの強力な次世代クラウドサンドボックス機能を企業ネットワーク外の環境からでも有効になりました。今後、ThreatSyncがHost
Sensorから不審なエンドポイント上のデータを受信した場合、マルウェアサンプルのハッシュを分析し、既存の脅威に関する膨大なデータライブラリと照合します。適合するデータがライブラリ上に存在しなかった場合、TDRはそれをクラウドサンドボックスであるAPT
Blockerと連携し、フルシステムエミュレーション環境で、きめ細かな分析が自動的に行われ、不審なデータの振る舞いと特徴を分析します。APT
Blockerの分析が完了すると、ThreatSyncに結果が反映され、脅威スコアがアップデートされた後に適切な処置が施されます。

TDRは包括的なクラウドベースソリューションとして、一元管理の元に直感性に優れたインターフェースを提供し、顧客の現場で新たな機能追加やトラブルシューティングに時間をかけることなく、膨大な数のサブスクリプションサービスを管理できるようになります。TDRはウォッチガードのTotal Security
Suiteに含まれており、例えばMSSPは他社ソリューションと差別化を図り、ビジネスの拡大に寄与することができます。1つのSKU、1つライセンスで、さらに充実した標的型攻撃の検知・レスポンスサービスを一貫して提供することにより、新たなビジネスチャンスを生み出すことに貢献します。

TDRはウォッチガードのTotal Security Suiteの一部として利用可能です。Host
Sensorのライセンス数はFireboxモデルにより異なり、アドオンオプションとしてセンサパッケージを追加購入することもできます。詳細は www.watchguard.co.jp/TDR をご覧下さい。

関連資料
・ TDRデータシート
・ TDRの技術概要
・ Host Sensorデータシート
・ ThreatSync機能概要
・ eBook：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
・ ホワイトペーパー：WatchGuard Threat Detection and Response による、既知、未知、回避型の脅威からの防御（英語）

【WatchGuard Technologiesについて】
WatchGuard (R) Technologiesは、業界標準ハードウェア、ベストオブブリードセキュリティ、ポリシーベースの管理ツールを独自アーキテクチャにより統合したビジネス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として、全世界の企業にエンタープライズクラスのセキュリティソリューションを提供しています。本社を米国ワシントン州シアトルに置き、北米、ヨーロッパ、アジア太平洋地区、中南米に支社を展開しています。日本法人であるウォッチガード・テクノロジー・ジャパン株式会社は、多くのパートナーを通じて、アプライアンス製品、ネットワークからエンドポイントまでの脅威検知とセキュリティの「可視化」及びセキュリティとネットワークの「運用管理」など拡大するニーズへのソリューションを提供しています。詳細は http://www.watchguard.co.jp をご覧下さい。

さらなる詳細情報、プロモーション活動、最新動向はTwitter（@WatchGuardJapan）、facebook（@WatchGuard.jp）、をフォローして下さい。また、最新の脅威に関するリアルタイム情報やその対策法はセキュリティセンターまでアクセスして下さい。
セキュリティセンター：https://www.watchguard.co.jp/security-center

WatchGuardは、WatchGuard Technologies, Inc.の登録商標です。その他の商標は各社に帰属します。

【本プレスリリースに関するお問合せ】
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
マーケティング担当：角田・堀江
Tel： 03-5797-7205
Fax： 03-5797-7207
Email： jpnsales@watchguard.com
URL： http://www.watchguard.co.jp

Generated by ぷれりりプレスリリース
https://www.prerele.com